PUBLIC VERSION

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

PASAFESHARE LLC, Plaintiff, v. MICROSOFT CORPORATION, Defendant.	C.A. No. 6:20-cv-00397-ADA Jury Trial Demanded

AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff paSafeShare LLC ("paSafeShare"), by and through its undersigned counsel, files this Amended Complaint against Microsoft Corporation ("Microsoft") for patent infringement of United States Patent Nos. 9,455,961, 9,615,116, and 10,095,848 (collectively, the "patents-in-suit") and alleges as follows:

NATURE OF THE ACTION

1. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1 *et seq.*

THE PARTIES

2. Plaintiff paSafeShare LLC is a New Jersey limited liability company having its principal place of business at 1 Shawnee Court, Colts Neck, New Jersey 07722.

3. On information and belief, Defendant Microsoft Corporation is a corporation organized and existing under the laws of the State of Washington with its principal place of business located at One Microsoft Way, Redmond, WA 98052. Microsoft may be served with process through its registered agent for service in Texas: Corporation Service Company, 211 East 7th Street, Suite 620, Austin, Texas 78701.

4. On information and belief, since at least November 1993, Microsoft has been registered to do business in the State of Texas under Texas SOS File Number 0010404606.

JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a) because this action arises under the patent laws of the United States, 35 U.S.C. §§ 1 *et seq.*

6. Microsoft is subject to this Court's personal jurisdiction in accordance with due process and/or the Texas Long Arm Statute because, in part, Microsoft "[r]ecruits Texas residents, directly or through an intermediary located in this state, for employment inside or outside this state." *See* Tex. Civ. Prac. & Rem. Code § 17.042.

7. Microsoft has already submitted to the jurisdiction of this Court in patent litigations bearing docket numbers: 6:19-cv-00399-ADA and 1:19-cv-00874-ADA.

8. This Court has personal jurisdiction over Microsoft because Microsoft (directly and/or through its subsidiaries, affiliates, or intermediaries) has committed and continues to commit acts of direct and indirect infringement in this judicial district in violation of at least 35 U.S.C. §§ 271(a) and (b). In particular, Microsoft makes, uses,

sells, offers for sale, and/or imports software products, systems, offerings, and/or services that infringe the patents-in-suit. Microsoft also induces others to use the infringing products, systems, offerings, and/or services.

9. This Court also has personal jurisdiction over Microsoft because Microsoft has sufficient minimum contacts with this forum as a result of business conducted within the State of Texas and this judicial district. In particular, this Court has personal jurisdiction over Microsoft because, *inter alia*, Microsoft, on information and belief: (1) has substantial, continuous, and systematic contacts with this State and this judicial district; (2) owns, manages, and operates facilities in this State and this judicial district; (3) enjoys substantial income from its operations and sales in this State and this judicial district; (4) employs Texas residents in this State and this judicial district, and (5) solicits business and markets products, offerings, systems and/or services in this State and this judicial district including, without limitation, related to the accused products, offerings, systems, and/or services.

10. Microsoft has purposefully availed itself of the privileges of conducting business within this judicial district; has established sufficient minimum contacts with this judicial district such that it should reasonably and fairly anticipate being hauled into court in this judicial district; has purposefully directed activities at residents of this judicial district; and at least a portion of the patent infringement claims alleged in this Complaint arise out of or are related to one or more of the foregoing activities.

11. Venue is proper in this judicial district pursuant to 28 U.S.C. § § 1391 (b)-(d) and/or 1400(b). Microsoft is registered to do business in the State of Texas, maintains

a regular and established place of business within this judicial district, and has committed acts of infringement in this judicial district.

12. On information and belief, Microsoft maintains a significant physical presence in this judicial district, including its corporate sales office locations, retail store locations, and datacenter locations.

13. On information and belief, Microsoft operates multiple corporate sales offices in this judicial district including, without limitation, offices located at 10900 Stonelake Boulevard, Suite 225, Austin, TX, USA 78759,[1] and Concord Park II, 401 East Sonterra Boulevard, Suite 300, San Antonio, TX, USA 78258.[2]

14. On information and belief, Microsoft markets, offers to sell, and/or sells products through its corporate sales offices located in this judicial district including, but not limited to, the accused products, offerings, systems, and/or services.

15. On information and belief, Microsoft operates multiple retail stores in this judicial district including, without limitation, stores located at 3309 Esperanza Crossing, Suite 104, Austin, TX, USA 78758,[3] and 15900 La Cantera Parkway, Suite 6560, San Antonio, TX, USA 78256.[4]

16. On information and belief, Microsoft maintains a list of certified learning partners in this judicial district that offer training solutions and certification in

[1] *See* https://www.microsoft.com/en-us/about/officelocator?Location=78258.
[2] *See* https://www.microsoft.com/en-us/about/officelocator?Location=78258.
[3] *See* https://www.microsoft.com/en-us/about/officelocator?Location=78258.
[4] *See* https://www.microsoft.com/en-us/about/officelocator?Location=78258.

Microsoft technology.[5] For example, on information and belief, at the ONLC Training Center, 700 Lavaca Street, Suite 1400, Austin, Texas 78701, Microsoft Certified Trainers offer training and courses in Microsoft Azure Security Technologies.[6]

17. On information and belief, Microsoft has spent at least tens of millions of dollars on networking and server infrastructure to support Microsoft Azure located in the State of Texas and in this judicial district.

18. On information and belief, Microsoft owns and operates multiple datacenters in this judicial district including, without limitation, data centers located at 5150 Rogers Road, San Antonio, TX 78251; 5200 Rogers Rd, San Antonio, TX 78251; 3823 Weisman Blvd, San Antonio, TX 78251; and 15000 Lambda Drive, San Antonio, TX 782245 (collectively, "Microsoft's Datacenter Locations").

19. On information and belief, Microsoft's Azure global infrastructure includes 58 regions worldwide. On information and belief, one of those regions is known as the "South Central US."

[5] *See* https://www.microsoft.com/en-us/learning/partners.aspx.
[6] *See* https://www.onlc.com/training/azure/austin-downtown-tx.htm.

See https://azure.microsoft.com/en-us/global-infrastructure/regions/.

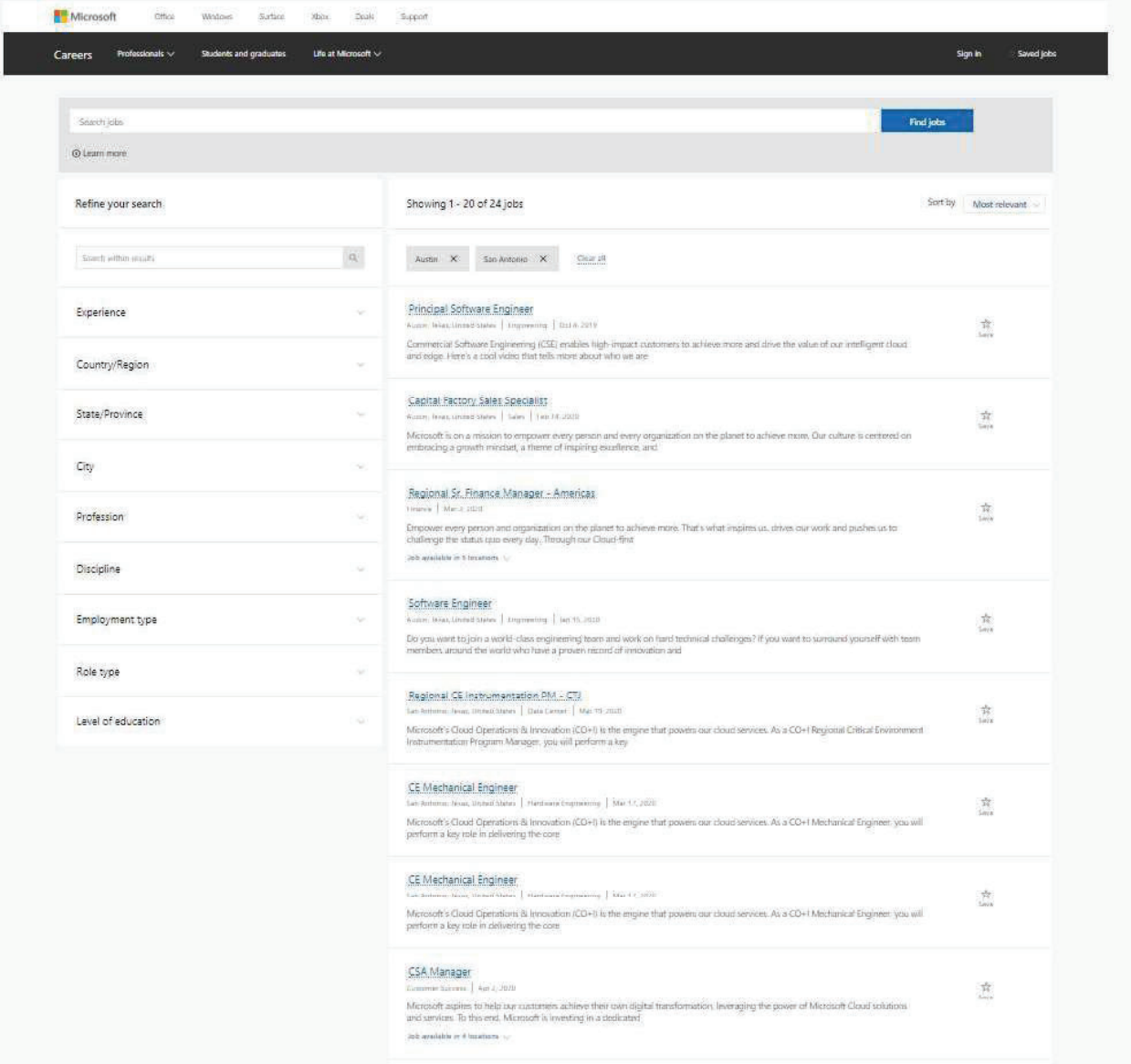
20. Microsoft provides a list of Azure products and services available in the "South Central US" region including, but not limited to, Azure Information Protection. *See* https://azure.microsoft.com/en-us/global-infrastructure/services/?regions=non-regional,us-south-central&products=all.

21. On information and belief, a substantial portion of the "South Central US" region's Azure network and server infrastructure is housed and operated in Microsoft's Datacenter Locations.

22. On information and belief, Microsoft has 36 H-1B labor condition applications for people employed in Austin, Texas.[7] On information and belief, Microsoft has 17 H-1B labor condition applications for people employed in San Antonio, Texas.[8] Employees holding an H-1B visa are employed in a specialty occupation that requires "theoretical and practical application of a body of highly specialized knowledge . . . and attainment of a bachelor's or higher degree in the specific specialty." *See generally* 8 U.S.C. § 1184. As such, Microsoft employees in Austin, Texas and San Antonio, Texas are highly specialized and important to the operation of Microsoft.

23. At the time of filing this lawsuit, Microsoft listed job openings on its website for positions in this judicial district.

[7] *See* https://h1bsalary.online/index.php?searchtext=MICROSOFT+CORPORATION&year=&minsalary=&state=&worksite_city=AUSTIN%2CTX&job_title=.
[8] *See* https://h1bsalary.online/index.php?searchtext=MICROSOFT+CORPORATION&year=&minsalary=&state=&worksite_city=San+Antonio&job_title=.



https://careers.microsoft.com/us/en/c/data-center-jobs (visited on 4/9/2020); *see also* https://jobs.careers.microsoft.com/global/en/search?q=azure&lc=Austin%2C%20Texas%2C%20United%20States&l=en_us&pg=1&pgSz=20&o=Relevance&flt=true (last visited 6/19/2023).

BACKGROUND

24. The patents-in-suit are the result of paSafeShare's years of research, design, and development of innovative and proprietary content distribution technologies.

25. Dr. Madhav S. Phadke and Kedar M. Phadke, co-inventors of the patents-in-suit, have over 50 years of combined experience in software development and technical consulting.

26. Dr. Madhav S. Phadke is a recognized leader in engineering design optimization and test methods. In the late 1980s, Dr. Phadke authored the first engineering textbook on robust design methods in the United States, *Quality Engineering Using Robust Design* (Prentice Hall, 1989). Dr. Phadke is also an ASQ Fellow and a recipient of the 2011 IEEE Region 1 Innovation Award.

27. In 1990, Dr. Phadke founded Phadke Associates, Inc. ("Phadke Associates"), a global consultancy and software services company. Phadke Associates develops and markets software tools for systems engineering process improvement and design and test optimization. Prior to founding Phadke Associates, Dr. Phadke was a manager in AT&T Bell Labs, a visiting scientist at the IBM Watson Research Center, and a Research Associate at the Army Math Research Center.

28. Dr. Phadke's son, Kedar M. Phadke, joined the family business in 2004 as Vice President of Phadke Associates. Mr. Phadke holds a Bachelor of Science in Economics from the Wharton School, University of Pennsylvania.

29. While working at Phadke Associates, the father-son duo noticed a significant oversight in existing content distribution security. In particular, they realized that while sensitive data could be protected by various security techniques (e.g., password-protected documents, access restricted web portals), there was no way to protect unwanted distribution by the recipient of the data.

30. In 2010, Dr. Madhav and Kedar Phadke founded paSafeShare LLC to address the deficiencies in existing content distribution security.

31. In or around mid-2010, Dr. Madhav and Kedar Phadke began developing technology related to secure content distribution.

32. The patents-in-suit were the result of their work.

33. paSafeShare did not sell or offer to sell any products or services that were covered by the claims of the patents-in-suit. Thus, paSafeShare did not have anything to mark pursuant to 35 U.S.C. § 287.

MICROSOFT'S WILLFUL INFRINGEMENT

34. On information and belief, in 2012, Microsoft sponsored an Accelerator program related to Microsoft Azure and solicited applications from companies to disclose their technology to Microsoft with the promise of a potential investment.[9] Microsoft specifically discouraged applicants from asking Microsoft to sign a non-disclosure agreement.[10]

35. paSafeShare applied to the Accelerator program in 2012 and provided Microsoft with information about its technology. On information and belief, Scott Guthrie was involved in the Accelerator program to which paSafeShare applied.[11]

---

[9] *See* https://web.archive.org/web/20120420232606/http://www.microsoft.com/BizSpark/accelerator/azure/default.aspx.

[10] *See* https://web.archive.org/web/20120421224403/http://www.microsoft.com/bizspark/accelerator/azure/faq.aspx.

[11] *See* https://weblogs.asp.net/scottgu/finalists-for-the-microsoft-accelerator-for-windows-azure.

36. After reviewing paSafeShare's technical information and its application to the Accelerator program, on July 26, 2012, Microsoft notified paSafeShare that it had been selected as a semi-finalist and solicited additional information from paSafeShare.

37. Shortly before or after receiving notice of its advancement as a semi-finalist in the Accelerator program, paSafeshare and Microsoft had a call in which they discussed the value proposition of paSafeShare's technology to Azure. After Microsoft informed paSafeShare of the type of "investment" Microsoft would be willing to make in paSafeShare, paSafeShare did not view Microsoft's proposal to be of any value to paSafeShare and, thus, paSafeShare withdrew from the program.

38. In January 2019, paSafeShare hired Brad Holtzinger of Tortuga Pacific to license or sell the patents-in-suit.

39. On information and belief, between July 2019 and December 2019, Mr. Holtzinger and/or Tortuga Pacific (on behalf of paSafeShare) contacted numerous Microsoft employees about paSafeShare and/or the patents-in-suit including Micky Minhas (Vice President, Associate General Counsel, Patents); Danielle Johnston Holmes (Associate General Counsel, Patent Group); Kurt DelBene (Executive Vice President, Corporate Strategy, Core Services Engineering and Operations); Scott Guthrie (Executive Vice President, Microsoft Cloud + AI Group); Qudus Olaniran (Senior Corporate Counsel); and Bahram Ali (Principal Patent Engineer).

40. On information and belief, Messrs. Olaniran and Ali both dealt with [redacted] as part of their job at Microsoft and worked on patent matters related to Azure hardware. Messrs. Olaniran and Ali both have

knowledge of patents and patent infringement as well as how to read patent specifications and claims. As part of his job at Microsoft, Mr. Ali worked with Microsoft's patent counsel [redacted].

43. Thus, by November 9, 2019, Mr. Holtzinger was a person known to both Messrs. Olaniran and Ali.

44. On November 9, 2019, believing that Microsoft may be interested in licensing or acquiring the patents-in-suit and knowing that both Messrs. Olaniran and Ali deal with [redacted] for Microsoft, Mr. Holtzinger sent Messrs. Olaniran and Ali an email, attaching a presentation about paSafeShare and the patents-

[12] Software runs on Azure hardware.

in-suit. The presentation identified each of the patents-in-suit by patent number, provided an overview of what each patent covered, and provided a general discussion of paSafeShare's patented technology.

45. Mr. Ali's email showed the November 9, 2019 email as being "read" by him. Messrs. Olaniran and Ali testified that they have no reason to believe that they did not review the email and the attached paSafeShare presentation, which identified the patents-in-suit.

46. According to Mr. Ali, emails such as the November 9, 2019 email would be considered an unsolicited email. [redacted]

47. On December 9, 2019, Mr. Holtzinger (on behalf of paSafeShare) sent a follow-up email to Messrs. Olaniran and Ali. The title of the follow-up email was "paSafeShare portfolio"; the email again attached the same presentation that was sent to Messrs. Olaniran and Ali on November 9, 2019.

48. Having heard nothing from Microsoft for months, in May 2020, paSafeShare sued Microsoft for patent infringement for Microsoft's unauthorized use of the patents-in-suit. Thus, by no later than November 2019, Microsoft engineers and lawyers had knowledge of the patents-in-suit and knew, or should have known, of Microsoft's infringement of the patents-in-suit. And, by no later than May 2020,

Microsoft had explicit notice of its infringement from paSafeShare's allegations. Despite its knowledge of the patents-in-suit and specific allegations of infringement for more than three years, Microsoft has continued its infringement and continued development and/or evolution of its infringing products, systems, offerings, and/or services.

49. After Microsoft had knowledge of paSafeShare's patents, Microsoft continued to use the infringing technology when it knew or should have known that its conduct infringed each of the patents-in-suit.

THE ASSERTED PATENTS

United States Patent No. 9,455,961

50. On September 27, 2016, the United States Patent and Trademark Office ("USPTO") duly and legally issued United States Patent No. 9,455,961 ("the '961 patent") entitled "System, Method and Apparatus for Securely Distributing Content" to inventors Madhav S. Phadke and Kedar M. Phadke.

51. The '961 patent is presumed valid under 35 U.S.C. § 282.

52. paSafeShare owns all rights, title, and interest in the '961 patent.

United States Patent No. 9,615,116

53. On April 4, 2017, the USPTO duly and legally issued United States Patent No. 9,615,116 ("the '116 patent) entitled "System, Method and Apparatus for Securely Distributing Content" to inventors Madhav S. Phadke and Kedar M. Phadke.

54. The '116 patent is presumed valid under 35 U.S.C. § 282.

55. paSafeShare owns all rights, title and interest in the '116 patent.

U.S. Patent No. 10,095,848

56. On October 9, 2018, the USPTO duly and legally issued United States Patent No. 10,095,848 ("the '848 patent) entitled "System, Method and Apparatus for Securely Distributing Content" to inventors Madhav S. Phadke and Kedar M. Phadke.

57. The '848 patent is presumed valid under 35 U.S.C. § 282.

58. paSafeShare owns all rights, title and interest in the '848 patent.

CLAIMS FOR RELIEF

Count I – Infringement of United States Patent No. 9,455,961

59. paSafeShare repeats, realleges, and incorporates by reference, as if fully set forth here, the preceding paragraphs of this Complaint.

60. Microsoft makes, uses, sells, offers for sale, and/or imports products, systems, offerings, and/or services for securely generating, distributing, and/or consuming protected content (e.g., documents and emails).

61. On April 17 and 19, 2023, paSafeShare served its final infringement contentions related to the '961 patent, which are incorporated here by reference.

62. Microsoft makes, uses, sells, offers to sell, and/or imports (1) computer software products, systems, offerings, and/or services (as well as associated servers) including, but not limited to, Microsoft Purview Information Protection, Purview Message Encryption, Purview Advanced Message Encryption, Microsoft Office Message Encryption (OME), Microsoft Information Protection, Azure Information Protection ("AIP"), Azure Rights Management, web portals for managing document protection (including, without limitation, the Purview web portal), and/or Microsoft client applications/modules/plug-ins (e.g., OfficeClient, AIP unified labeling client,

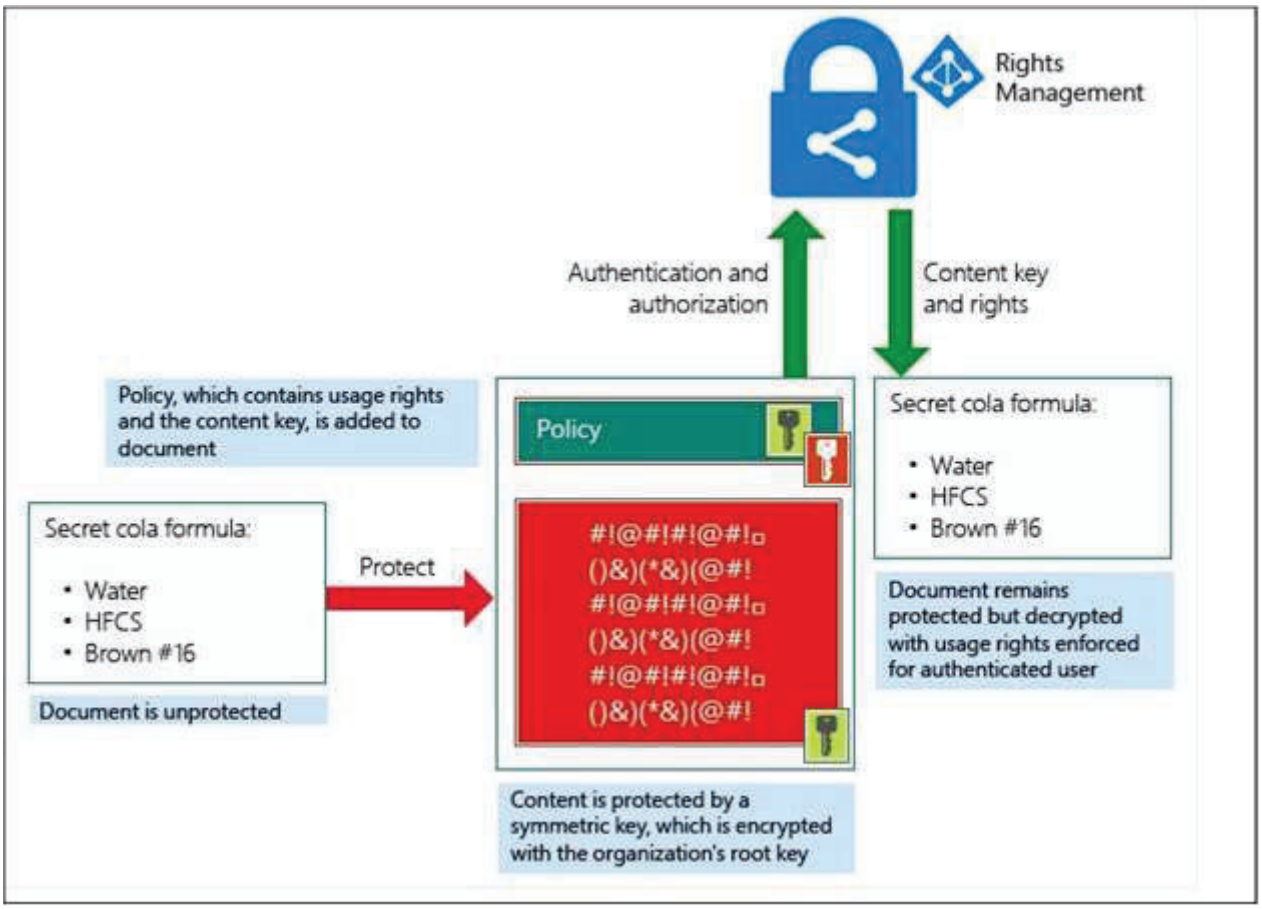
RMS client (e.g., Microsoft MSIPC), Microsoft Adobe Acrobat plug-ins) and (2) certain other Microsoft products (including, but not limited to, those that are considered "RMS-enlightened" applications) that are used with or work with the products, systems, offerings, and/or services set forth in (1) in the protection of digital content including, but not limited to, Windows, Office 365 (academic, home, business, front line, enterprise, and/or government) (including, without limitation, Office 365 A3, A5, E3 and E5), Microsoft 365 (academic, home, business, front line, enterprise, and/or government) (including, without limitation, Microsoft 365 E3, E5, E5 compliance, G3, G5, F1, F3, F5 compliance, F5 security plus compliance), Word, Excel, PowerPoint, OneNote, Microsoft PDF reader, SharePoint, OneDrive, Outlook, Enterprise Mobility Plus Security E3 and E5, Microsoft cloud app security, Microsoft Defender for Cloud Apps, Microsoft Cloud App Security, Exchange server, Azure Information Protection scanner, and/or Microsoft software running on Android, macOS and/or iOS. The products, systems, offerings, and/or services in these two categories work together to provide platforms e.g., for generating, distributing, and/or consuming protected documents and emails (the "Microsoft Azure RMS Platforms").

63. The Microsoft Azure RMS Platforms infringe the '961 patent.

64. Microsoft sells and/or offers to sell access and/or licenses to the Microsoft Azure RMS Platforms.

65. On information and belief, the Microsoft Azure RMS Platforms practice a method for securely distributing content. Specifically, on information and belief, the

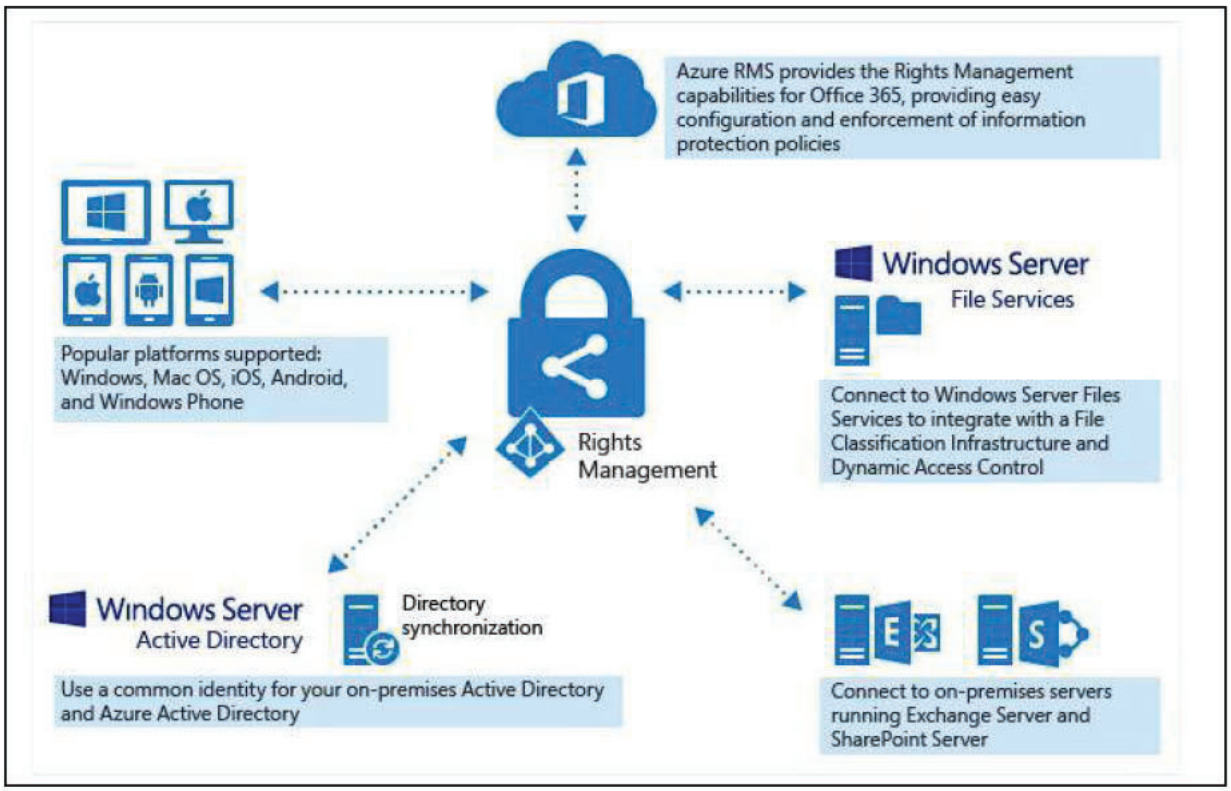
Microsoft Azure RMS Platforms use rights management technology to protect documents and emails using labels and policies defined by an administrator.[13]



How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

[13] *See* https://microsoft.github.io/AzureTipsAndTricks/blog/tip177.html.

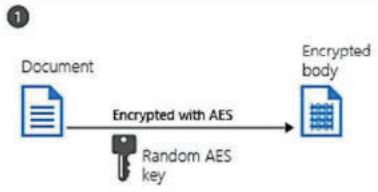
66. On information and belief, the Microsoft Azure RMS Platforms are cloud-based services.



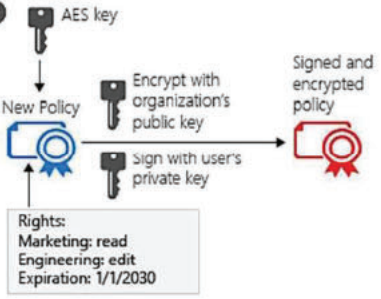
What is Azure Rights Management?, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/what-is-azure-rms (last visited April 2020).

67. On information and belief, the Microsoft Azure RMS Platforms generate, at a server (e.g., a Microsoft cloud server, a device running a Microsoft email application, or a server hosting a virtual desktop or web application environment that provides a user with access to Microsoft applications) in communication with a network (e.g., the Internet, a Microsoft network (e.g., Azure network), and/or a Microsoft customer network), a protected document package (PDP) (e.g., a data package that includes a protected document or protected email) including encrypted content or a

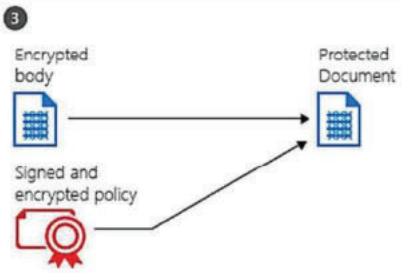
link to encrypted content (e.g., a document or email whose content has been encrypted), and a Publisher Key (PK) (e.g., a key and data regarding policy/use restrictions contained in a publishing license) for decrypting said encrypted content for presentation of said content by an authorized user via a Limited Capability Viewer (LCV) (a Microsoft application that enforces/applies/implements policy/use restrictions) (e.g., Microsoft Word, Excel, PowerPoint, OneNote, PDF viewer, AIP Viewer, OfficeClient, AIP unified labeling client, RMS client (e.g., Microsoft MSIPC), Outlook Desktop, Outlook Mac, Outlook Web Application (OWA), Outlook mobile applications, Microsoft Exchange, etc.).



What's happening in step 1: The RMS client creates a random key (the content key) and encrypts the document using this key with the AES symmetric encryption algorithm.



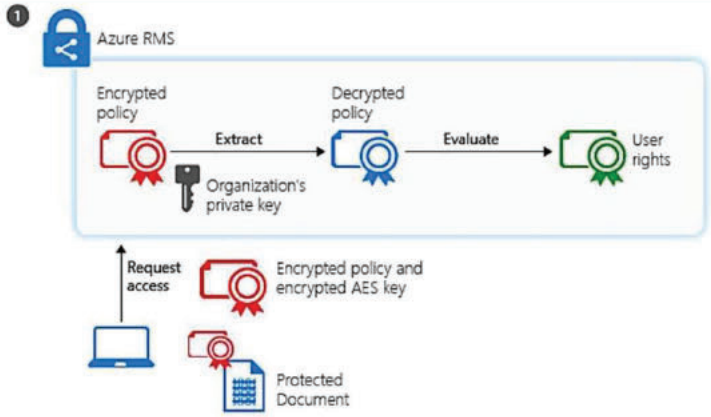
What's happening in step 2: The RMS client then creates a certificate that includes a policy for the document that includes the usage rights for users or groups, and other restrictions, such as an expiration date. These settings can be defined in a template that an administrator previously configured, or specified at the time the content is protected (sometimes referred to as an "ad hoc policy").



What's happening in step 3: Finally, the RMS client embeds the policy into a file with the body of the document encrypted previously, which together comprise a protected document.

How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

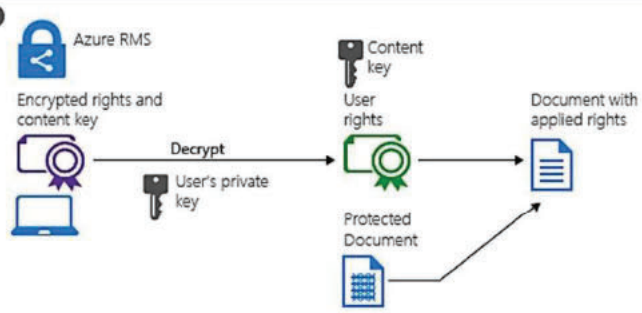
68. The Microsoft Azure RMS Platforms generate software instructions (e.g., (1) the file extension of the protected document/email, the metadata of the protected document/email, and the content of the publishing license other than the content of the publishing license that comprises the PK, or (2) the elements set forth in (1) *and* the label and/or markers of the compound file format of the protected document/email) that, when executed by a processor at a user device (e.g., personal computer, virtual desktop/server, mobile phone, tablet, server providing a web application, and/or Microsoft Exchange server) of a proposed authorized user (e.g., a user of a user device which has not received a UL for the protected document, and who has an email address that (1) is not an email address in the content owner's / sender's domain, and (2) has not been federated with the content owner's/sender's domain), cause the user device to generate a Content Consumer License Request (CCLR) (e.g., message/request sent to obtain a UL) identifying said PK.



What's happening in step 1: The authenticated user sends the document policy and the user's certificates to the Azure Rights Management service. The service decrypts and evaluates the policy, and builds a list of rights (if any) the user has for the document. To identify the user, the Azure AD ProxyAddresses attribute is used for the user's account and groups to which the user is a member. For performance reasons, group membership is cached. If the user account has no values for the Azure AD ProxyAddresses attribute, the value in the Azure AD UserPrincipalName is used instead.

How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

69. The authorized user comprises a user having a Content Consumer License (CCL) (e.g., use license / end user license) compatible with the PK to enable decryption of the encrypted content by the PK included within the PDP.



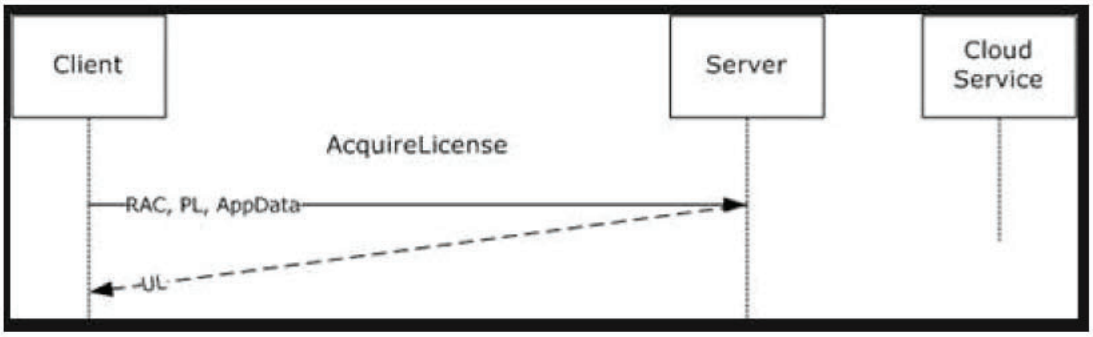
What's happening in step 3: Finally, the RMS client takes the encrypted use license and decrypts it with its own user private key. This lets the RMS client decrypt the document's body as it is needed and render it on the screen.

The client also decrypts the rights list and passes them to the application, which enforces those rights in the application's user interface.

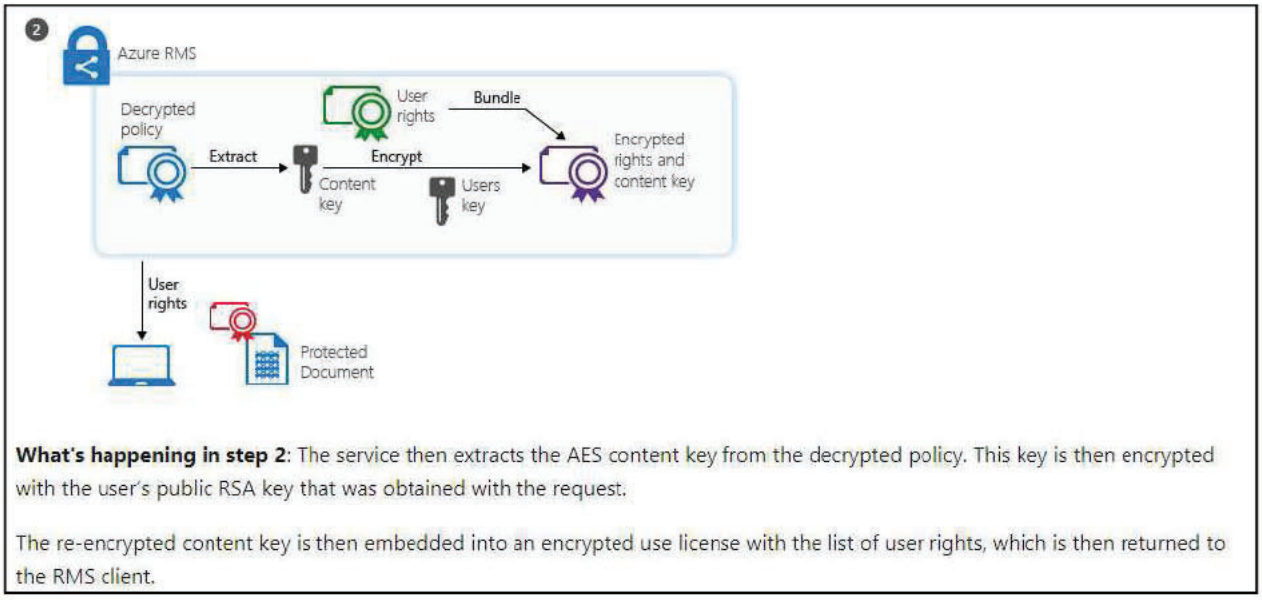
How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

70. The Microsoft Azure RMS Platforms propagate, via the network, the PDP toward at least one user.

71. In response to receiving from a proposed authorized user a CCLR identifying the PK, the Microsoft Azure RMS Platforms propagate a CCL compatible with the PK toward the proposed authorized user.



See https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-rmpr/2402901e-ee24-40fc-a480-5d007dbfdf57 (last visited June 2023).

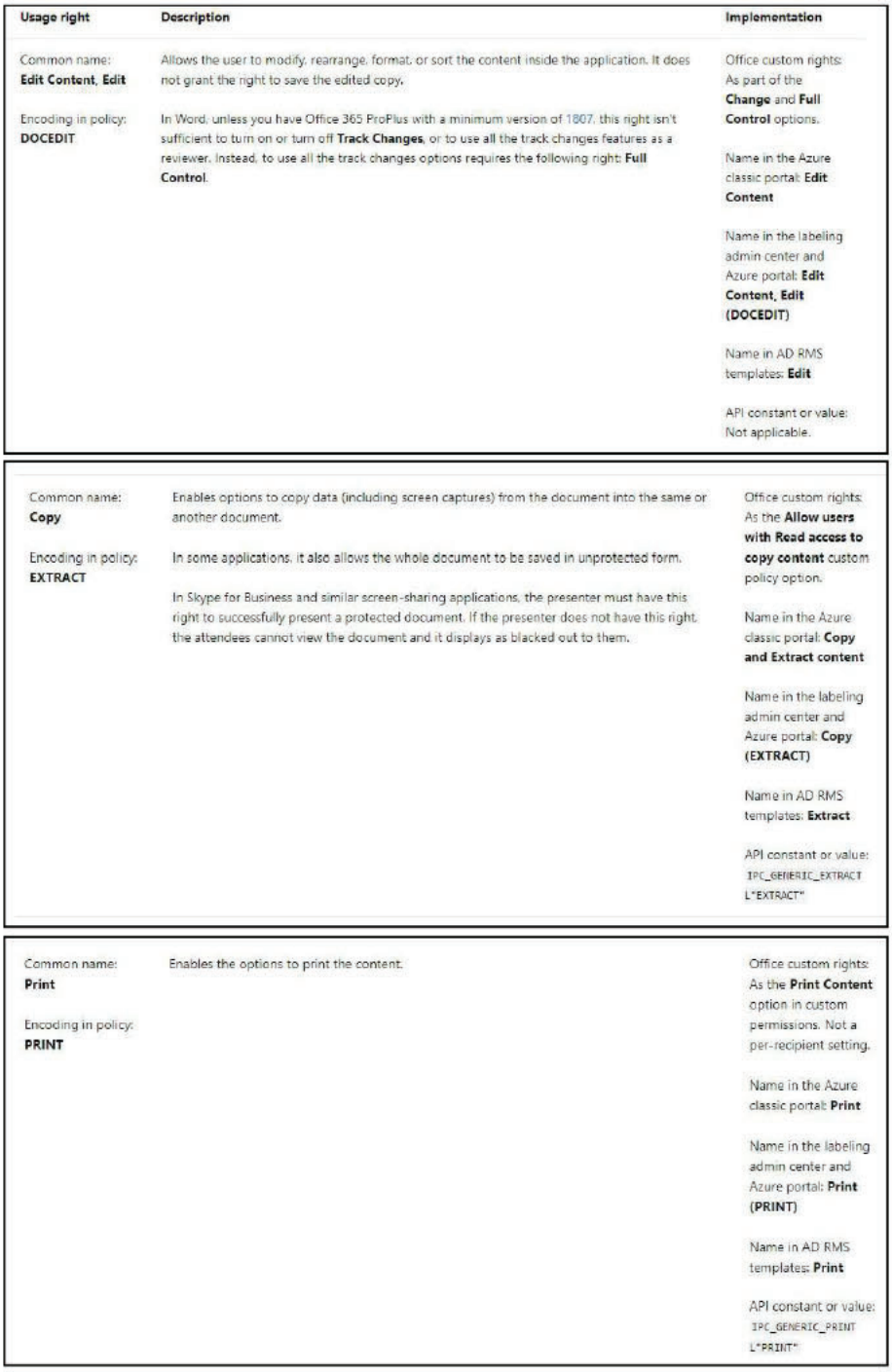


How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

72. The proposed authorized user is an unauthorized user where received PDP license requirements are not satisfied (e.g., when the device associated with the user does not have a UL enabling the user to consume the protected document/email).

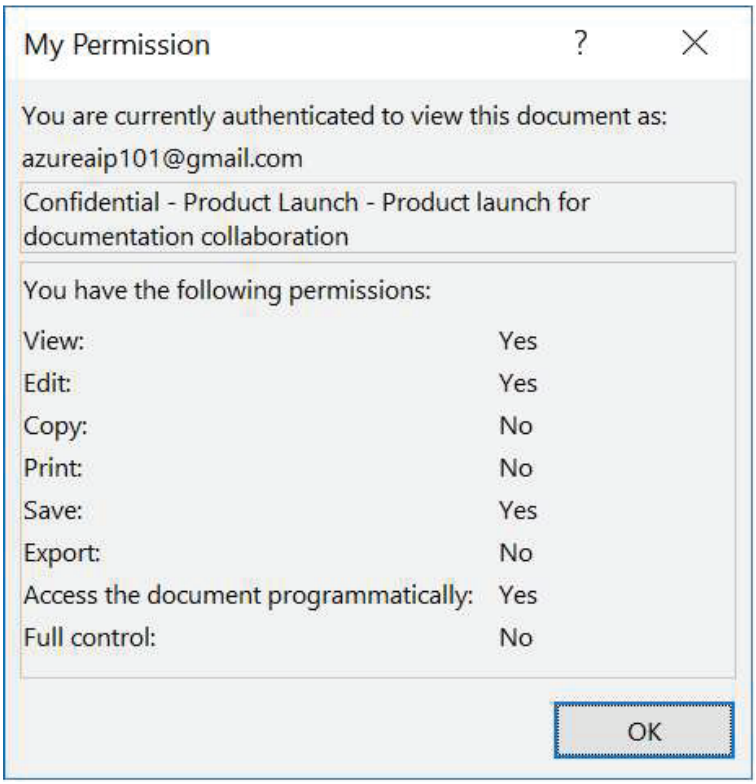
73. The LCV is configured to restrict editing, printing and copying of the

content.

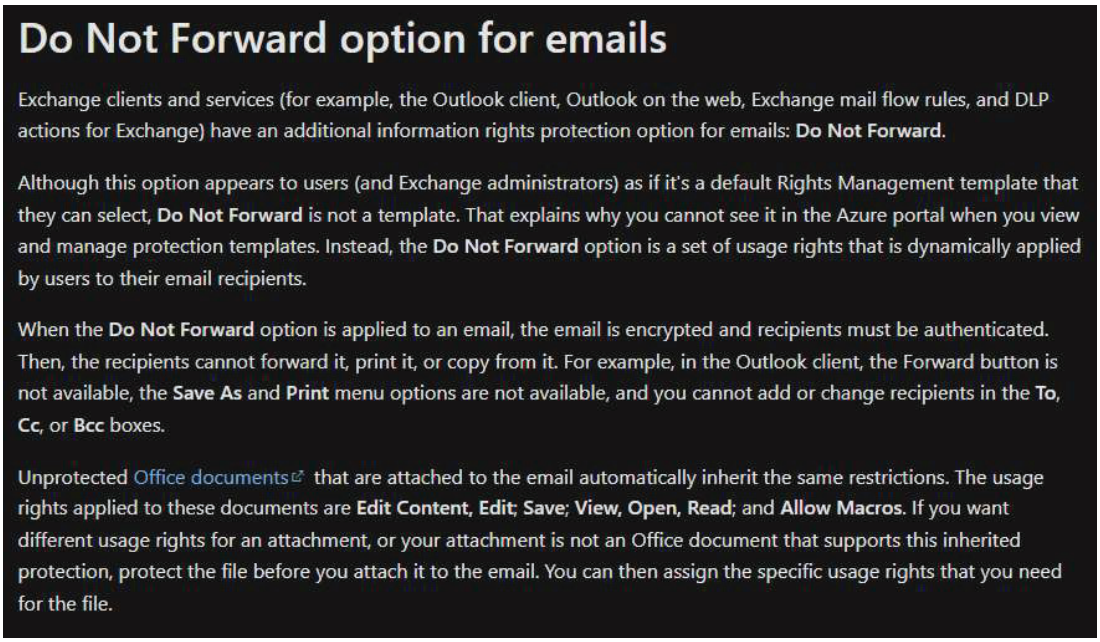


Usage right	Description	Implementation
Common name: **Edit Content, Edit** Encoding in policy: **DOCEDIT**	Allows the user to modify, rearrange, format, or sort the content inside the application. It does not grant the right to save the edited copy. In Word, unless you have Office 365 ProPlus with a minimum version of 1807, this right isn't sufficient to turn on or turn off **Track Changes**, or to use all the track changes features as a reviewer. Instead, to use all the track changes options requires the following right: **Full Control**.	Office custom rights: As part of the **Change** and **Full Control** options. Name in the Azure classic portal: **Edit Content** Name in the labeling admin center and Azure portal: **Edit Content, Edit (DOCEDIT)** Name in AD RMS templates: **Edit** API constant or value: Not applicable.
Common name: **Copy** Encoding in policy: **EXTRACT**	Enables options to copy data (including screen captures) from the document into the same or another document. In some applications, it also allows the whole document to be saved in unprotected form. In Skype for Business and similar screen-sharing applications, the presenter must have this right to successfully present a protected document. If the presenter does not have this right, the attendees cannot view the document and it displays as blacked out to them.	Office custom rights: As the **Allow users with Read access to copy content** custom policy option. Name in the Azure classic portal: **Copy and Extract content** Name in the labeling admin center and Azure portal: **Copy (EXTRACT)** Name in AD RMS templates: **Extract** API constant or value: `IPC_GENERIC_EXTRACT L"EXTRACT"`
Common name: **Print** Encoding in policy: **PRINT**	Enables the options to print the content.	Office custom rights: As the **Print Content** option in custom permissions. Not a per-recipient setting. Name in the Azure classic portal: **Print** Name in the labeling admin center and Azure portal: **Print (PRINT)** Name in AD RMS templates: **Print** API constant or value: `IPC_GENERIC_PRINT L"PRINT"`

Configuring Usage Rights For Azure Information Protection, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights (last visited April 2020).



See https://learn.microsoft.com/en-us/previous-versions/azure/information-protection/secure-collaboration-documents#opening-and-editing-the-protected-document (last visited June 2023).



Do Not Forward option for emails

Exchange clients and services (for example, the Outlook client, Outlook on the web, Exchange mail flow rules, and DLP actions for Exchange) have an additional information rights protection option for emails: **Do Not Forward**.

Although this option appears to users (and Exchange administrators) as if it's a default Rights Management template that they can select, **Do Not Forward** is not a template. That explains why you cannot see it in the Azure portal when you view and manage protection templates. Instead, the **Do Not Forward** option is a set of usage rights that is dynamically applied by users to their email recipients.

When the **Do Not Forward** option is applied to an email, the email is encrypted and recipients must be authenticated. Then, the recipients cannot forward it, print it, or copy from it. For example, in the Outlook client, the Forward button is not available, the **Save As** and **Print** menu options are not available, and you cannot add or change recipients in the **To**, **Cc**, or **Bcc** boxes.

Unprotected Office documents that are attached to the email automatically inherit the same restrictions. The usage rights applied to these documents are **Edit Content, Edit**; **Save**; **View, Open, Read**; and **Allow Macros**. If you want different usage rights for an attachment, or your attachment is not an Office document that supports this inherited protection, protect the file before you attach it to the email. You can then assign the specific usage rights that you need for the file.

See https://learn.microsoft.com/en-us/azure/information-protection/configure-usage-rights (last visited June 2023).

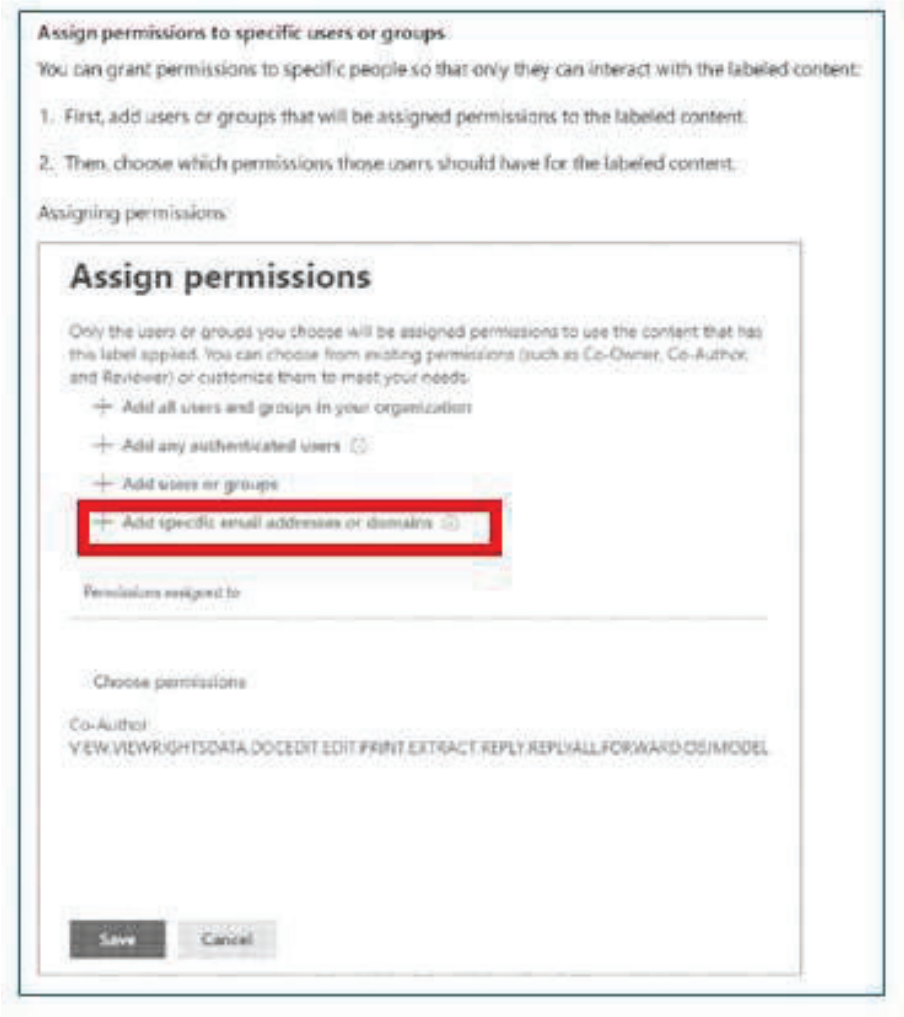
74. On information and belief, one or more Microsoft subsidiaries and/or affiliates use the Microsoft Azure RMS Platforms in regular business operations.

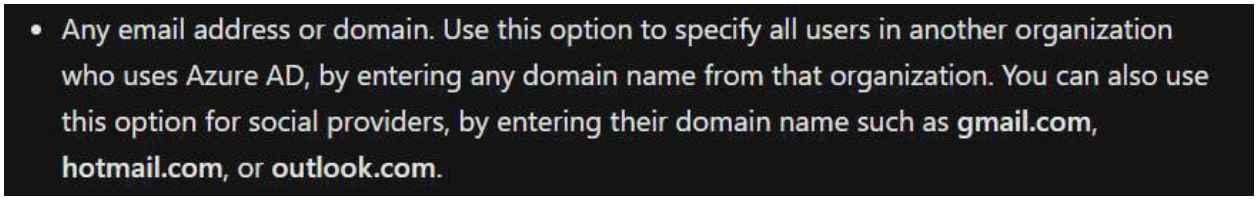
75. On information and belief, the Microsoft Azure RMS Platforms are available to businesses and individuals throughout the United States.

76. On information and belief, the Microsoft Azure RMS Platforms are provided to businesses and individuals located in the Western District of Texas.

77. On information and belief, Microsoft, without authorization or license, has been and continues to directly infringe (literally and/or under the doctrine of equivalents) at least claim 1 of the '961 patent by making, using, selling, offering for sale, and/or importing products, systems, offerings, and/or services for securely generating, distributing, and/or consuming protected content including, but not limited to, the Microsoft Azure RMS Platforms.

78. For example, in the context of protected documents on the Microsoft Azure RMS Platforms, specific email addresses or domains can be added to a rights policy template. Those email addresses are external to the organization of the content owner or sender (e.g., outside the content owner's/sender's domain) and have not been federated with the domain of the content owner/sender prior to sending the protected document. Thus, infringement occurs at least by Microsoft implementing the feature shown in the red box below.





See https://learn.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels?view=o365-worldwide#requirements-and-limitations-for-add-any-authenticated-users (last visited June 2023).

79. As another example, in the context of protected emails (including email attachments) on the Microsoft Azure RMS Platforms, specific email addresses or domains—which are external to the organization of the content owner or sender (e.g., outside the content owner's/sender's domain) and have not been federated with the domain of the content owner/sender—can be added to a rights policy template. Thus, infringement occurs at least by: (1) sending a protected email between a Microsoft email application (web, mobile, or desktop) and (a) a Microsoft email web application (e.g., Outlook web application (OWA)) or (b) a non-Microsoft application (e.g. Gmail, Yahoo! MacOS mail, and other web and/or desktop mail applications); or (2) sending a protected email between a Microsoft email application (web, mobile, or desktop) and a non-Microsoft mobile application (e.g. Gmail, iOS mail).

Situation	Legacy OME	IRM in AD RMS	Microsoft Purview Message Encryption
Sending an encrypted mail	Through Exchange mail flow rules	End-user initiated from Outlook desktop or Outlook on the Web; or through Exchange mail flow rules	End-user initiated from Outlook desktop, Outlook for Mac, or Outlook on the Web; through Exchange mail flow rules (also known as transport rules) and data loss prevention (DLP)
Rights management template	N/A	Do Not Forward option and custom templates	Do Not Forward option, encrypt-only option, and custom templates
Recipient type	Internal and external recipients	Internal recipients only	Internal and external recipients
Experience for internal recipient	Recipients receive an HTML message, which they download and open in a web browser or mobile app	Native inline experience in Outlook clients	Native inline experience for recipients in the same organization using Outlook clients. Recipients can read message from encrypted message portal using clients other than Outlook (no download or app required).
Experience for external recipient	Recipients receive an HTML message, which they download and open in a web browser or mobile app	N/A	Native inline experience for Microsoft 365 recipients. All other recipients can read message from OME portal (no download or app required).
Attachment permissions	No restrictions on attachments	Attachments are protected	Attachments are protected for the Do Not Forward option and custom templates. Admins can choose whether attachments for the encrypt-only option are protected or not.
Bring your own key (BYOK) support	None	None	BYOK supported

See https://learn.microsoft.com/en-us/microsoft-365/compliance/ome-version-comparison?view=o365-worldwide (last visited June 2023).

- **Email protection**: When Exchange Online and Office 365 Message Encryption with new capabilities is used to protect email messages, authentication for consumption can also use federation with a social identity provider or by using a one-time passcode. Then, the process flows are very similar, except that content consumption happens service-side in a web browser session over a temporarily cached copy of the outbound email.

See https://learn.microsoft.com/en-us/azure/information-protection/how-does-it-work (last visited June 2023).

See https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/secure-email-recommended-policies?view=o365-worldwide (last visited June 2023).

80. By making, using, offering for sale, selling, and/or importing products, systems, offerings, and/or services for securely generating, distributing, and/or consuming protected content (including, but not limited to, the Microsoft Azure RMS Platforms), Microsoft has injured paSafeShare and is liable to the Plaintiff for directly infringing one or more claims of the '961 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a).

81. On information and belief, Microsoft also indirectly infringes the '961 patent by actively inducing infringement under 35 USC § 271(b).

82. Microsoft has been on notice of the '961 patent at least since November 9, 2019.

83. On information and belief, Microsoft intends/intended to induce patent infringement by third-party customers and users of the Microsoft Azure RMS Platforms and has/had knowledge that its inducing acts cause/would cause infringement or

is/was willfully blind to the possibility that its inducing acts cause/would cause infringement.

84. On information and belief, Microsoft specifically intends and is aware that the normal and customary use of the accused products infringe the '961 patent. Microsoft performs the acts that constitute induced infringement, and induce actual infringement, with knowledge of the '961 patent and with the knowledge that the induced acts constitute infringement. For example, Microsoft provides the infringing Microsoft Azure RMS Platforms, and further provides documentation and training materials that cause customers and end users of the Microsoft Azure RMS Platforms to use the products in a manner that directly infringe one or more claims of the '961 patent. By providing instruction and training to customers and end users on how to use the Microsoft Azure RMS Platforms in a manner that directly infringes one or more claims of the '961 patent, including at least claim 1, Microsoft specifically intends to induce infringement of the '961 patent. On information and belief, Microsoft engages in such inducement (e.g., through Microsoft user manuals, product support, marketing materials, and training materials to actively induce the users of the Microsoft Azure RMS Platforms to infringe the '961 patent) to promote the sales of the Microsoft Azure RMS Platforms. Accordingly, Microsoft has induced and continues to induce users of the Microsoft Azure RMS Platforms to use the Microsoft Azure RMS Platforms in their ordinary and customary way to infringe the '961 patent, knowing that such use constitutes infringement of the '961 patent.

85. Microsoft's infringement of the '961 patent was and continues to be willful.

86. Microsoft's direct and/or indirect infringement has damaged paSafeShare and paSafeShare is suffering and will continue to suffer irreparable harm and damages as a result of this infringement.

Count II – Infringement of United States Patent No. 9,615,116

87. paSafeShare repeats, realleges, and incorporates by reference, as if fully set forth here, the preceding paragraphs of this Complaint.

88. Microsoft makes, uses, sells, offers for sale, and/or imports products, systems, offerings, and/or services for securely generating, distributing, and/or consuming protected content (e.g., documents and emails).

89. On April 17 and 19, 2023, paSafeShare served its final infringement contentions related to the '116 patent, which are incorporated here by reference.

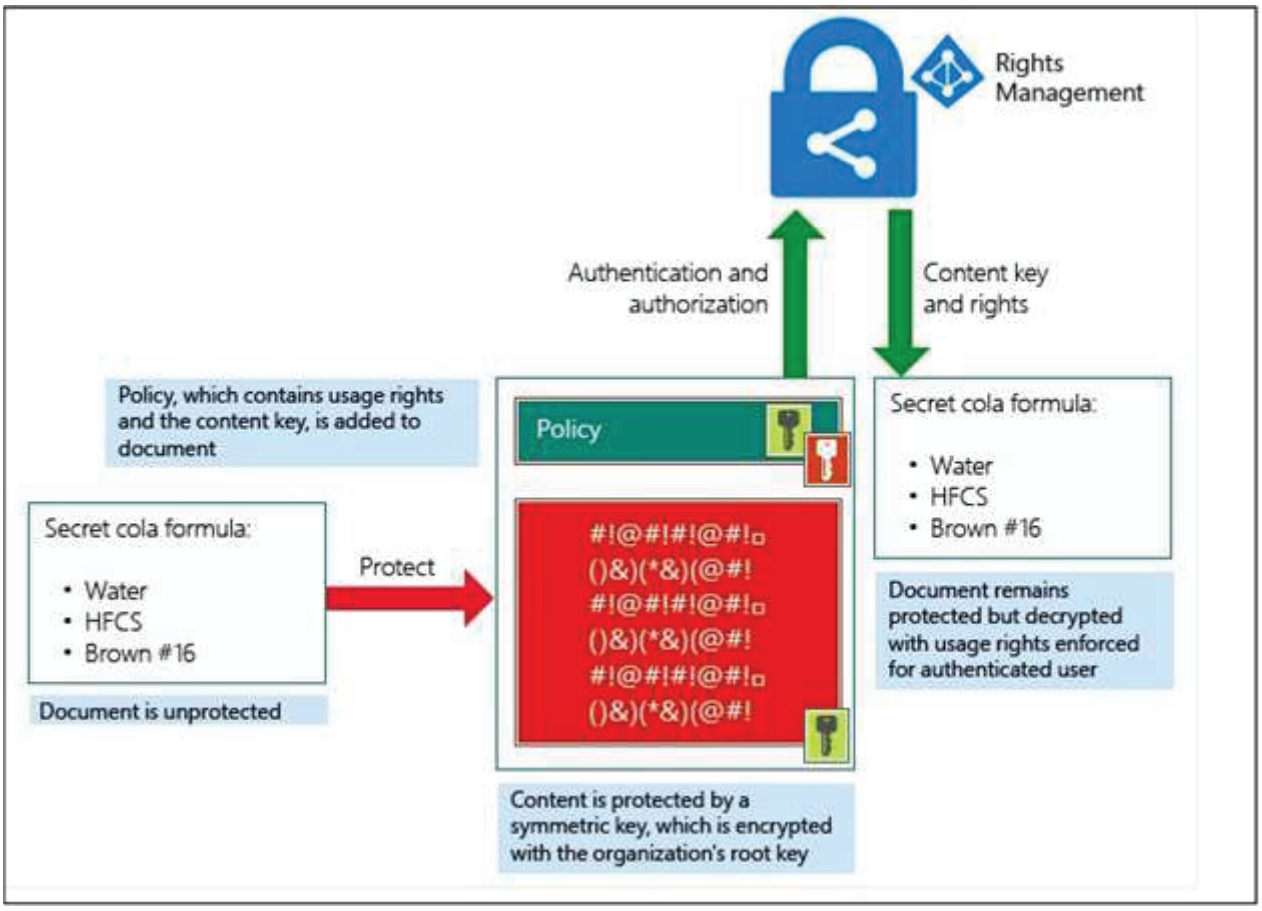
90. Microsoft makes, uses, sells, offers to sell, and/or imports the Microsoft Azure RMS Platforms.

91. The Microsoft Azure RMS Platforms infringe the '116 patent.

92. Microsoft sells and/or offers to sell access and/or licenses to the Microsoft Azure RMS Platforms.

93. On information and belief, the Microsoft Azure RMS Platforms practice a method for securely distributing content. Specifically, on information and belief, the

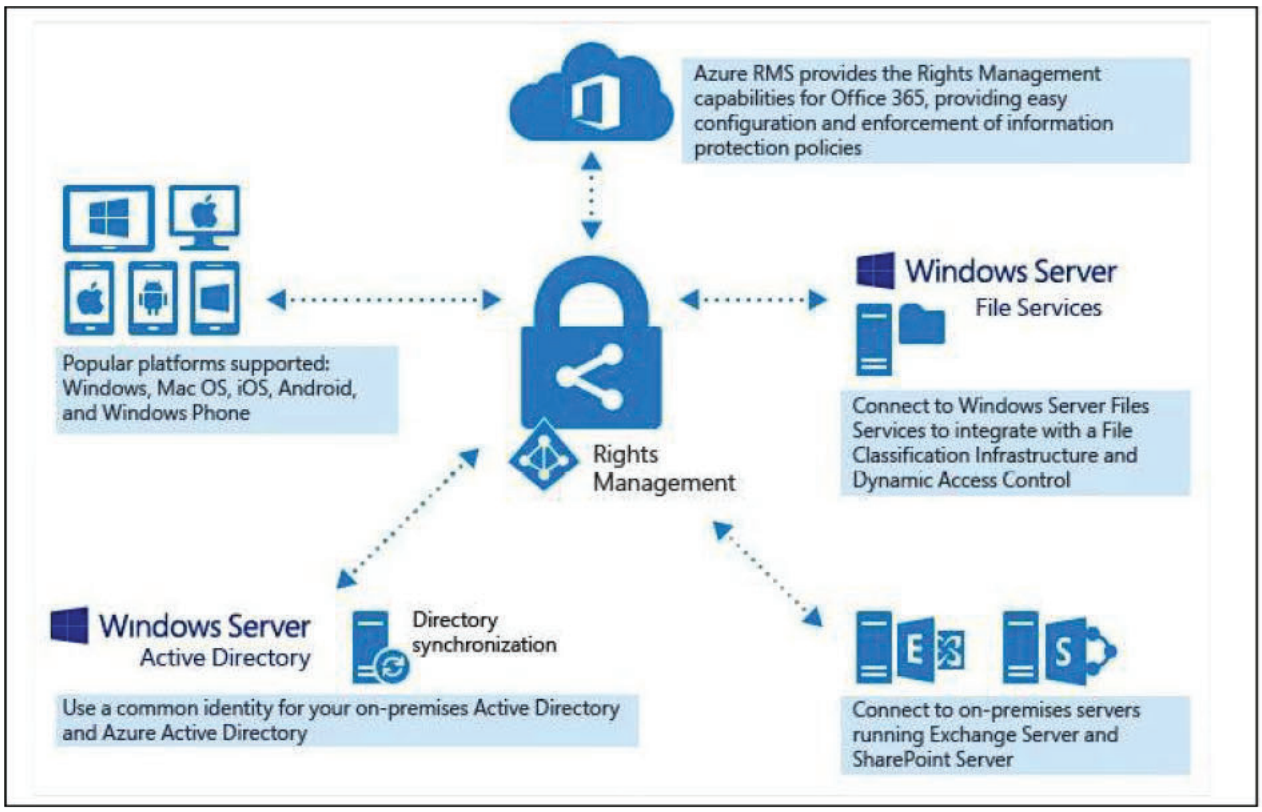
Microsoft Azure RMS Platforms use rights management technology to protect documents and emails using labels and policies defined by an administrator.[14]



How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en- us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure- rms-works-first-use-content-protection-content-consumption (last visited April 2020).

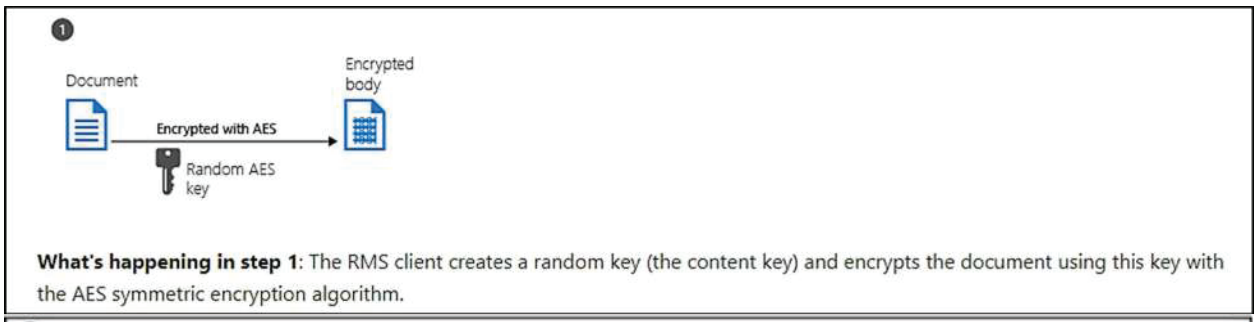
94. On information and belief, the Microsoft Azure RMS Platforms are cloud-based services.

[14] *See* https://microsoft.github.io/AzureTipsAndTricks/blog/tip177.html.



What is Azure Rights Management?, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/what-is-azure-rms (last visited April 2020).

95. On information and belief, the Microsoft Azure RMS Platforms generate, at a server (e.g., a Microsoft cloud server, a device running a Microsoft email application, or a server hosting a virtual desktop or web application environment that provides a user with access to Microsoft applications), a protected document package (PDP) (e.g., a data package that includes a protected document or protected email), the PDP including encrypted content (e.g., a document or email whose content has been encrypted), and a Publisher Key (PK) (e.g., a key and data regarding policy/use restrictions contained in a publishing license) associated with the encrypted content.



What's happening in step 1: The RMS client creates a random key (the content key) and encrypts the document using this key with the AES symmetric encryption algorithm.

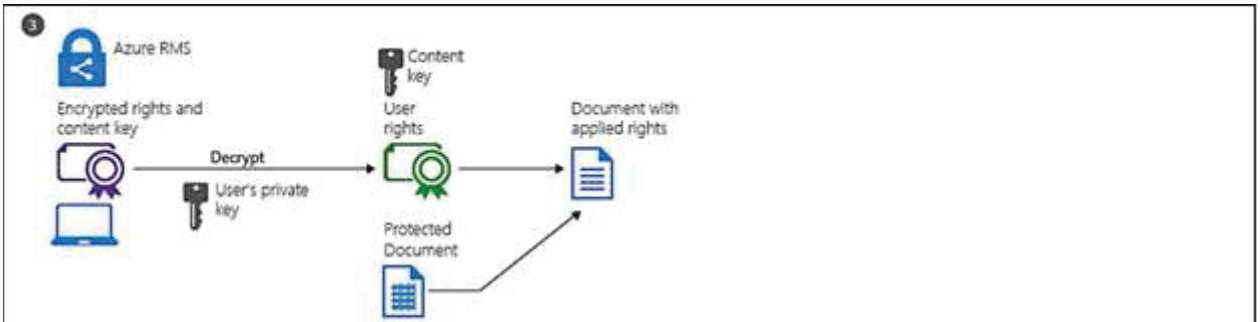
What's happening in step 2: The RMS client then creates a certificate that includes a policy for the document that includes the usage rights for users or groups, and other restrictions, such as an expiration date. These settings can be defined in a template that an administrator previously configured, or specified at the time the content is protected (sometimes referred to as an "ad hoc policy").

What's happening in step 3: Finally, the RMS client embeds the policy into a file with the body of the document encrypted previously, which together comprise a protected document.

How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

96. The PK enables decryption of the encrypted content for presentation via a Limited Capability Viewer (LCV) (a Microsoft application that enforces/applies/implements policy/use restrictions) (e.g., Microsoft Word, Excel, PowerPoint, OneNote, PDF viewer, AIP Viewer, OfficeClient, AIP unified labeling

client, RMS client (e.g., Microsoft MSIPC), Outlook Desktop, Outlook Mac, Outlook Web Application (OWA), Outlook mobile applications, Microsoft Exchange, etc.) of an authorized user device (e.g. a device (e.g. laptop, desktop, mobile phone, tablet, server/virtual desktop) that has received a use license (UL) for the protected document/email).



What's happening in step 3: Finally, the RMS client takes the encrypted use license and decrypts it with its own user private key. This lets the RMS client decrypt the document's body as it is needed and render it on the screen.

The client also decrypts the rights list and passes them to the application, which enforces those rights in the application's user interface.

How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

97. The authorized user device comprises a user device having a Content Consumer License (CCL) (e.g., use license / end user license) compatible with the PK to enable presentation via the LCV of locally stored encrypted content (e.g. protected content stored on a user device) from the PDP.

Rights Management use license

When a user opens a document or email that has been protected by Azure Rights Management, a Rights Management use license for that content is granted to the user. This use license is a certificate that contains the user's usage rights for the document or email message, and the encryption key that was used to encrypt the content. The use license also contains an expiry date if this has been set, and how long the use license is valid.

A user must have a valid use license to open the content in addition to their rights account certificate (RAC), which is a certificate that's granted when the user environment is initialized and then renewed every 31 days.

For the duration of the use license, the user is not reauthenticated or reauthorized for the content. This lets the user continue to open the protected document or email without an internet connection. When the use license validity period expires, the next time the user accesses the protected document or email, the user must be reauthenticated and reauthorized.

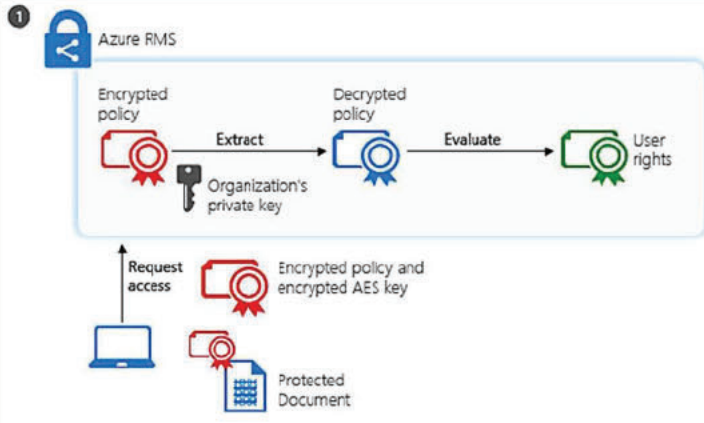
When documents and email messages are protected by using a label or a template that defines the protection settings, you can change these settings in your label or template without having to reprotect the content. If the user has already accessed the content, the changes take effect after their use license has expired. However, when users apply custom permissions (also known as an ad-hoc rights policy) and these permissions need to change after the document or email is protected, that content must be protected again with the new permissions. Custom permissions for an email message are implemented with the Do Not Forward option.

The default use license validity period for a tenant is 30 days and you can configure this value by using the PowerShell cmdlet, Set-AipServiceMaxUseLicenseValidityTime. You can configure a more restrictive setting for when protection is applied by using a label or template:

Configuring Usage Rights for Azure Information Protection, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights (last visited April 2020).

98. The PDP includes software instructions (e.g., (1) the file extension of the protected document/email, the metadata of the protected document/email, and the content of the publishing license other than the content of the publishing license that comprises the PK, or (2) the elements set forth in (1) *and* the label and/or markers of the compound file format of the protected document/email) that, when executed by a processor at a proposed authorized user device (e.g. device of a user (e.g., laptop, desktop, mobile phone, tablet, server providing web application, virtual desktop/server) which has not received a UL for the protected document/email, and which corresponds to a user having an email address that (1) is not an email address in

the content owner's / sender's domain, and (2) has not been federated with the content owner's/sender's domain), cause the proposed authorized user device to generate a Content Consumer License Request (CCLR) (e.g., message/request sent to obtain a UL) identifying the PK.

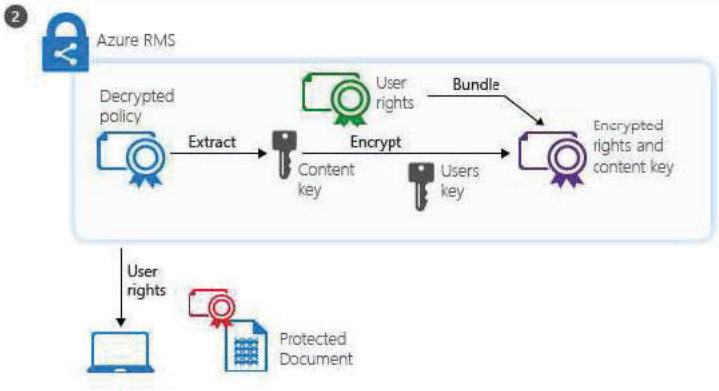


What's happening in step 1: The authenticated user sends the document policy and the user's certificates to the Azure Rights Management service. The service decrypts and evaluates the policy, and builds a list of rights (if any) the user has for the document. To identify the user, the Azure AD ProxyAddresses attribute is used for the user's account and groups to which the user is a member. For performance reasons, group membership is cached. If the user account has no values for the Azure AD ProxyAddresses attribute, the value in the Azure AD UserPrincipalName is used instead.

How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

99. The Microsoft Azure RMS Platforms propagate the PDP toward at least one authorized or proposed authorized user device.

100. The Microsoft Azure RMS Platforms receive from a proposed authorized user device having the PDP a CCLR identifying the PK.

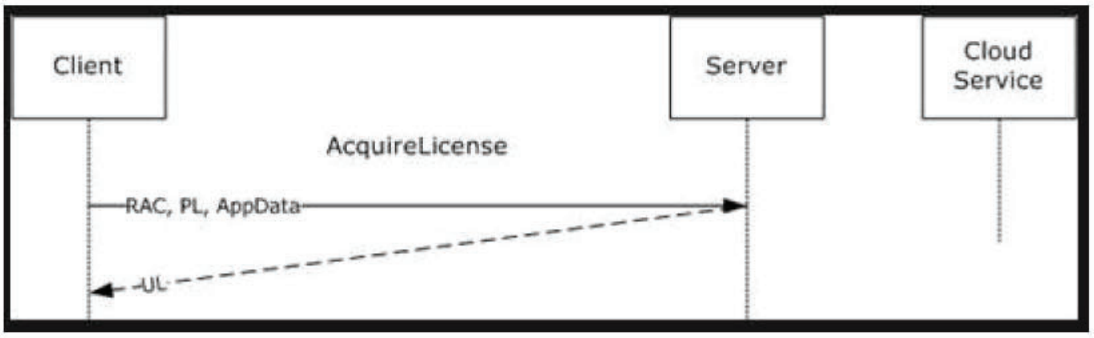


What's happening in step 2: The service then extracts the AES content key from the decrypted policy. This key is then encrypted with the user's public RSA key that was obtained with the request.

The re-encrypted content key is then embedded into an encrypted use license with the list of user rights, which is then returned to the RMS client.

How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

101. The Microsoft Azure RMS Platforms propagate a CCL (e.g., use license / end user license) compatible with the PK toward the proposed authorized user device if the CCLR is valid.



See https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-rmpr/2402901e-ee24-40fc-a480-5d007dbfdf57 (last visited June 2023).

102. On information and belief, one or more Microsoft subsidiaries and/or affiliates use the Microsoft Azure RMS Platforms in regular business operations.

103. On information and belief, the Microsoft Azure RMS Platforms are available to businesses and individuals throughout the United States.

104. On information and belief, the Microsoft Azure RMS Platforms are provided to businesses and individuals located in the Western District of Texas.

105. On information and belief, Microsoft, without authorization or license, has been and continues to directly infringe (literally and/or under the doctrine of equivalents) at least claim 1 of the '116 patent by making, using, selling, offering for sale, and/or importing products, systems, offerings, and/or services for securely generating, distributing, and/or consuming protected content including, but not limited to, the Microsoft Azure RMS Platforms.

106. For example, in the context of protected documents on the Microsoft Azure RMS Platforms, specific email addresses or domains can be added to a rights policy template. Those email addresses are external to the organization of the content owner or sender (e.g., outside the content owner's/sender's domain) and have not been federated with the domain of the content owner/sender prior to sending the protected document. Thus, infringement occurs at least by Microsoft implementing the feature shown in the red box below.

- Any email address or domain. Use this option to specify all users in another organization who uses Azure AD, by entering any domain name from that organization. You can also use this option for social providers, by entering their domain name such as **gmail.com**, **hotmail.com**, or **outlook.com**.

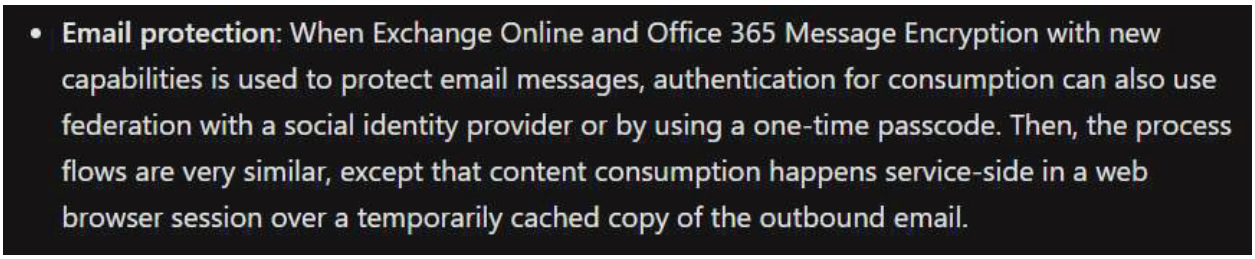
See https://learn.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels?view=o365-worldwide#requirements-and-limitations-for-add-any-authenticated-users (last visited June 2023).

107. As another example, in the context of protected emails (including email attachments) on the Microsoft Azure RMS Platforms, specific email addresses or domains—which are external to the organization of the content owner or sender (e.g.,

outside the content owner's/sender's domain) and have not been federated with the domain of the content owner/sender—can be added to a rights policy template. Thus, infringement occurs at least by: (1) sending a protected email between a Microsoft email application (web, mobile, or desktop) and (a) a Microsoft email web application (e.g., Outlook web application (OWA)) or (b) a non-Microsoft application (e.g. Gmail, Yahoo! MacOS mail, and other web and/or desktop mail applications); or (2) sending a protected email between a Microsoft email application (web, mobile, or desktop) and a non-Microsoft mobile application (e.g. Gmail, iOS mail).

Situation	Legacy OME	IRM in AD RMS	Microsoft Purview Message Encryption
Sending an encrypted mail	Through Exchange mail flow rules	End-user initiated from Outlook desktop or Outlook on the Web; or through Exchange mail flow rules	End-user initiated from Outlook desktop, Outlook for Mac, or Outlook on the Web; through Exchange mail flow rules (also known as transport rules) and data loss prevention (DLP)
Rights management template	N/A	Do Not Forward option and custom templates	Do Not Forward option, encrypt-only option, and custom templates
Recipient type	Internal and external recipients	Internal recipients only	Internal and external recipients
Experience for internal recipient	Recipients receive an HTML message, which they download and open in a web browser or mobile app	Native inline experience in Outlook clients	Native inline experience for recipients in the same organization using Outlook clients. Recipients can read message from encrypted message portal using clients other than Outlook (no download or app required).
Experience for external recipient	Recipients receive an HTML message, which they download and open in a web browser or mobile app	N/A	Native inline experience for Microsoft 365 recipients. All other recipients can read message from OME portal (no download or app required).
Attachment permissions	No restrictions on attachments	Attachments are protected	Attachments are protected for the Do Not Forward option and custom templates. Admins can choose whether attachments for the encrypt-only option are protected or not.
Bring your own key (BYOK) support	None	None	BYOK supported

See https://learn.microsoft.com/en-us/microsoft-365/compliance/ome-version-comparison?view=o365-worldwide (last visited June 2023).



See https://learn.microsoft.com/en-us/azure/information-protection/how-does-it-work (last visited June 2023).

See https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/secure-email-recommended-policies?view=o365-worldwide (last visited June 2023).

108. By making, using, offering for sale, selling, and/or importing products, systems, offerings, and/or services for securely generating, distributing, and/or consuming protected content (including, but not limited to, the Microsoft Azure RMS Platforms), Microsoft has injured paSafeShare and is liable to the Plaintiff for directly infringing one or more claims of the '116 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a)

109. On information and belief, Microsoft also indirectly infringes the '116

patent by actively inducing infringement under 35 USC § 271(b).

110. Microsoft has been on notice of the '116 patent at least since November 9, 2019.

111. On information and belief, Microsoft intends/intended to induce patent infringement by third-party customers and users of the Microsoft Azure RMS Platforms and has/had knowledge that its inducing acts cause/would cause infringement or is/was willfully blind to the possibility that its inducing acts cause/would cause infringement.

112. On information and belief, Microsoft specifically intends and is aware that the normal and customary use of the accused products infringe the '116 patent. Microsoft performs the acts that constitute induced infringement, and induces actual infringement, with knowledge of the '116 patent and with the knowledge that the induced acts constitute infringement. For example, Microsoft provides the infringing Microsoft Azure RMS Platforms, and further provides documentation and training materials that cause customers and end users of the Microsoft Azure RMS Platforms to use the products in a manner that directly infringe one or more claims of the '116 patent. By providing instruction and training to customers and end users on how to use the Microsoft Azure RMS Platforms in a manner that directly infringes one or more claims of the '116 patent, including at least claim 1, Microsoft specifically intends to induce infringement of the '116 patent. On information and belief, Microsoft engages in such inducement (e.g., through Microsoft user manuals, product support, marketing materials, and training materials to actively induce the users of the Microsoft Azure

RMS Platforms to infringe the '116 patent) to promote the sales of the Microsoft Azure RMS Platforms. Accordingly, Microsoft has induced and continues to induce users of the Microsoft Azure RMS Platforms to use the Microsoft Azure RMS Platforms in their ordinary and customary way to infringe the '116 patent, knowing that such use constitutes infringement of the '116 patent.

113. Microsoft's infringement of the '116 patent was and continues to be willful.

114. Microsoft's direct and/or indirect infringement has damaged paSafeShare, and Microsoft is suffering and will continue to suffer irreparable harm and damages as a result of this infringement.

Count III – Infringement of United States Patent No. 10,095,848

115. paSafeShare repeats, realleges, and incorporates by reference, as if fully set forth here, the preceding paragraphs of this Complaint.

116. Microsoft makes, uses, sells, offers for sale, and/or imports products, systems, offerings, and/or services for securely generating, distributing, and/or consuming protected content (e.g., documents and emails).

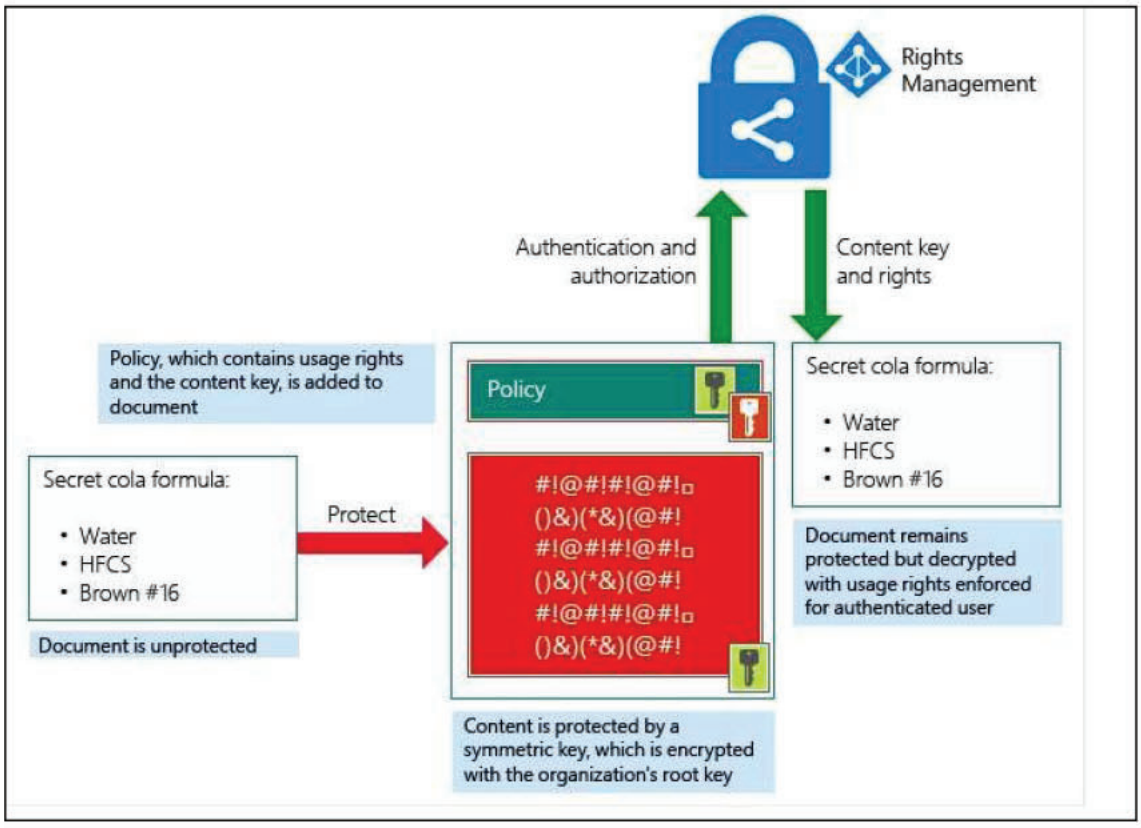
117. On April 17 and 19, 2023, paSafeShare served its final infringement contentions related to the '848 patent, which are incorporated here by reference.

118. Microsoft makes, uses, sells, offers to sell, and/or imports the Microsoft Azure RMS Platforms.

119. The Microsoft Azure RMS Platforms infringe the '848 patent.

120. Microsoft sells and/or offers to sell access and/or licenses to the Microsoft Azure RMS Platforms.

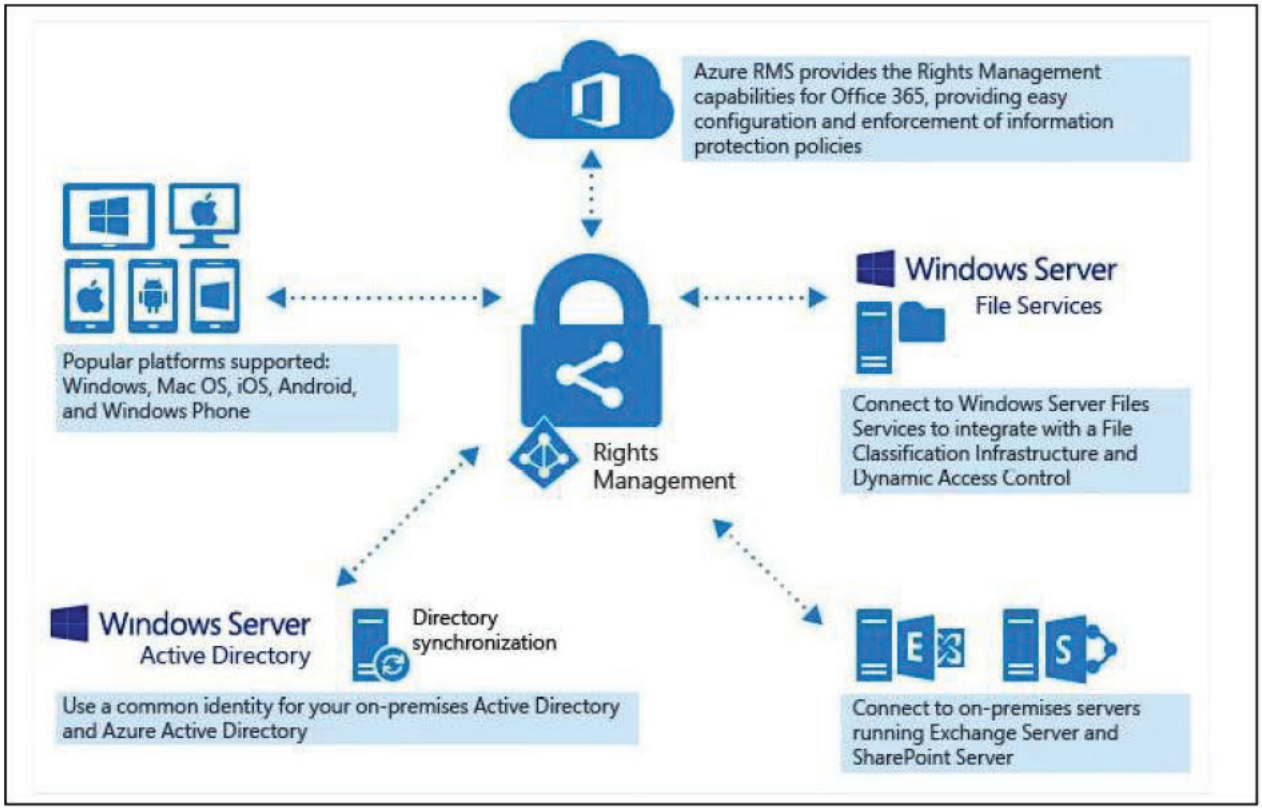
121. On information and belief, the Microsoft Azure RMS Platforms practice a method for securely distributing content. Specifically, on information and belief, the Microsoft Azure RMS Platforms use rights management technology to protect documents and emails using labels and policies defined by an administrator.[15]



How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

[15] *See* https://microsoft.github.io/AzureTipsAndTricks/blog/tip177.html.

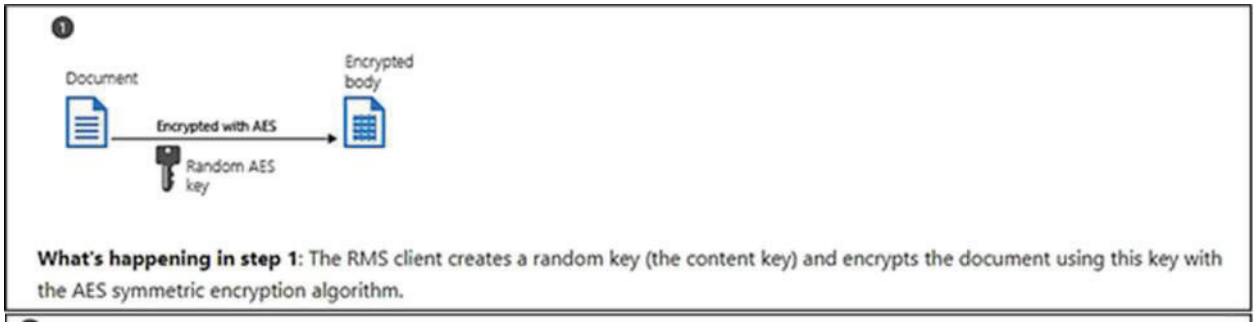
122. On information and belief, Microsoft Azure RMS Platforms are cloud-based services.



What is Azure Rights Management?, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/what-is-azure-rms (last visited April 2020).

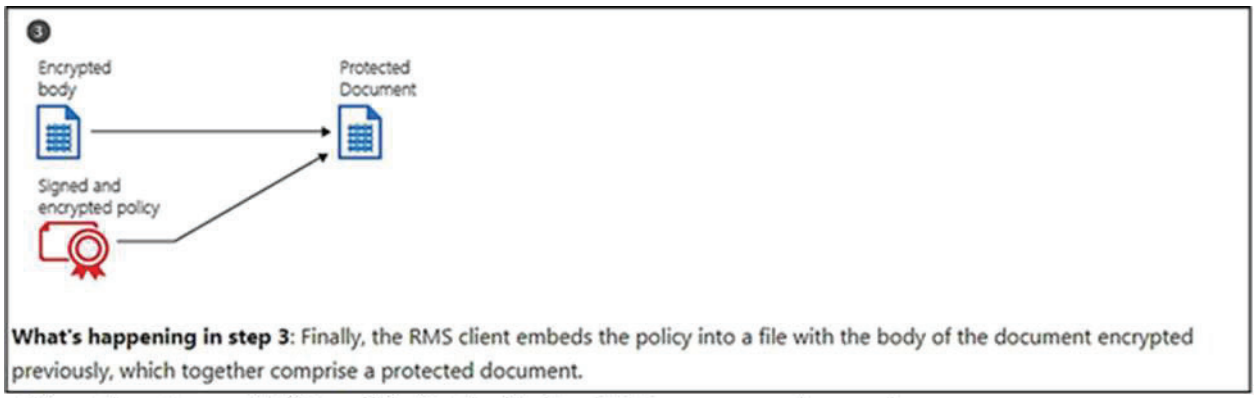
123. On information and belief, the Microsoft Azure RMS Platforms generate, at a server (e.g., a Microsoft cloud server, a device running a Microsoft email application, or a server hosting a virtual desktop or web application environment that provides a user with access to Microsoft applications) in communication with a network (e.g., the Internet, a Microsoft network (e.g., Azure network), and/or a Microsoft customer network), a protected document package (PDP) (e.g., a data package that includes a protected document or protected email) including encrypted content or a

link to encrypted content (e.g., a document or email whose content has been encrypted), and a Publisher Key (PK) (e.g., a key and data regarding policy/use restrictions contained in a publishing license) for decrypting said encrypted content for presentation of said content by an authorized user via a Limited Capability Viewer (LCV) (a Microsoft application that enforces/applies/implements policy/use restrictions) (e.g., Microsoft Word, Excel, PowerPoint, OneNote, PDF viewer, AIP Viewer, OfficeClient, AIP unified labeling client, RMS client (e.g., Microsoft MSIPC), Outlook Desktop, Outlook Mac, Outlook Web Application (OWA), Outlook mobile applications, Microsoft Exchange, etc.).



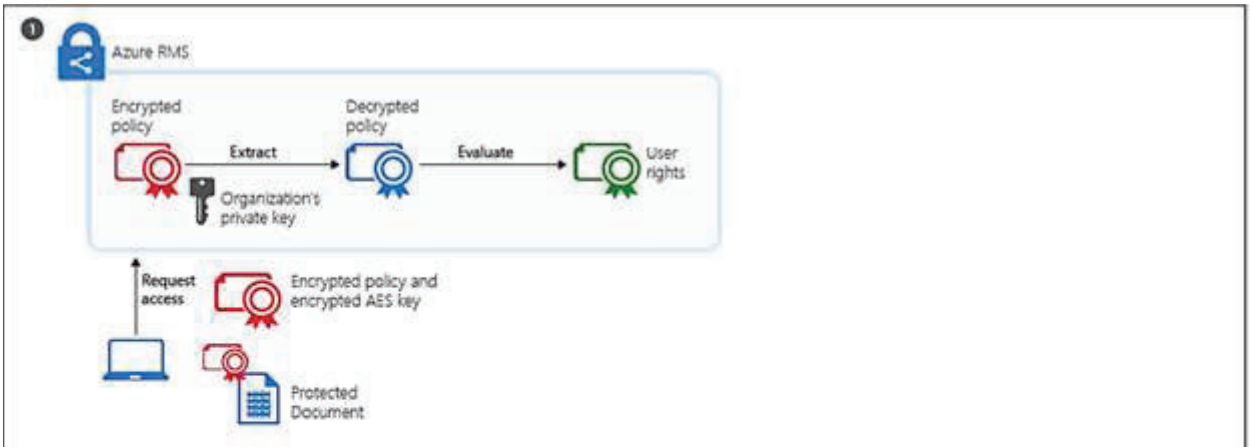
What's happening in step 1: The RMS client creates a random key (the content key) and encrypts the document using this key with the AES symmetric encryption algorithm.

What's happening in step 2: The RMS client then creates a certificate that includes a policy for the document that includes the usage rights for users or groups, and other restrictions, such as an expiration date. These settings can be defined in a template that an administrator previously configured, or specified at the time the content is protected (sometimes referred to as an "ad hoc policy").



How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

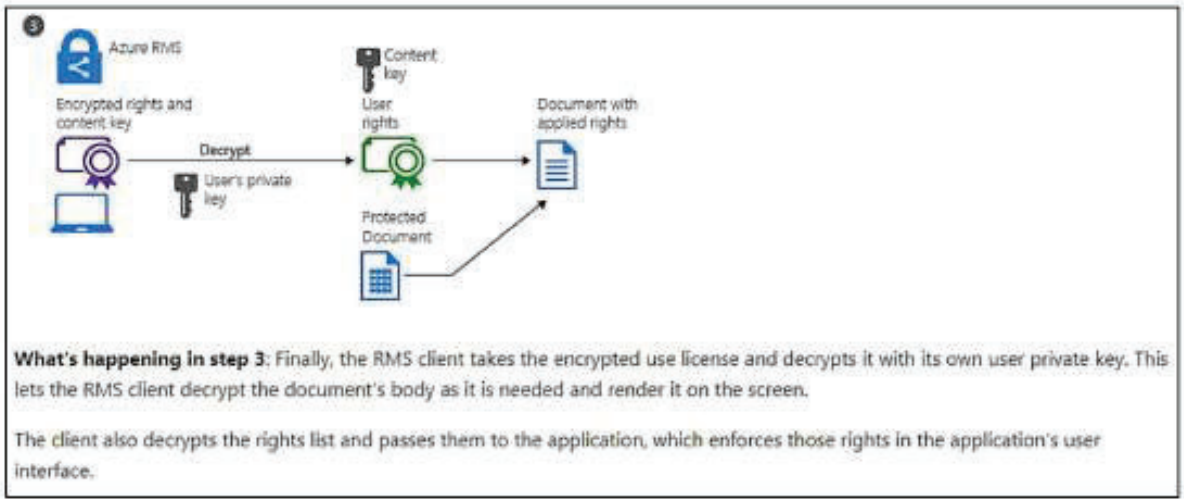
124. The Microsoft Azure RMS Platforms generate software instructions (e.g., (1) the file extension of the protected document/email, the metadata of the protected document/email, and the content of the publishing license other than the content of the publishing license that comprises the PK, or (2) the elements set forth in (1) *and* the label and/or markers of the compound file format of the protected document/email) that, when executed by a processor at a user device (e.g., personal computer, virtual desktop/server, mobile phone, tablet, server providing a web application, and/or Microsoft Exchange server) of a proposed authorized user (e.g., a user of a user device which has not received a UL for the protected document, and who has an email address that (1) is not an email address in the content owner's / sender's domain, and (2) has not been federated with the content owner's/sender's domain), cause the user device to generate a Content Consumer License Request (CCLR) (e.g., message/request sent to obtain a UL) identifying said PK.



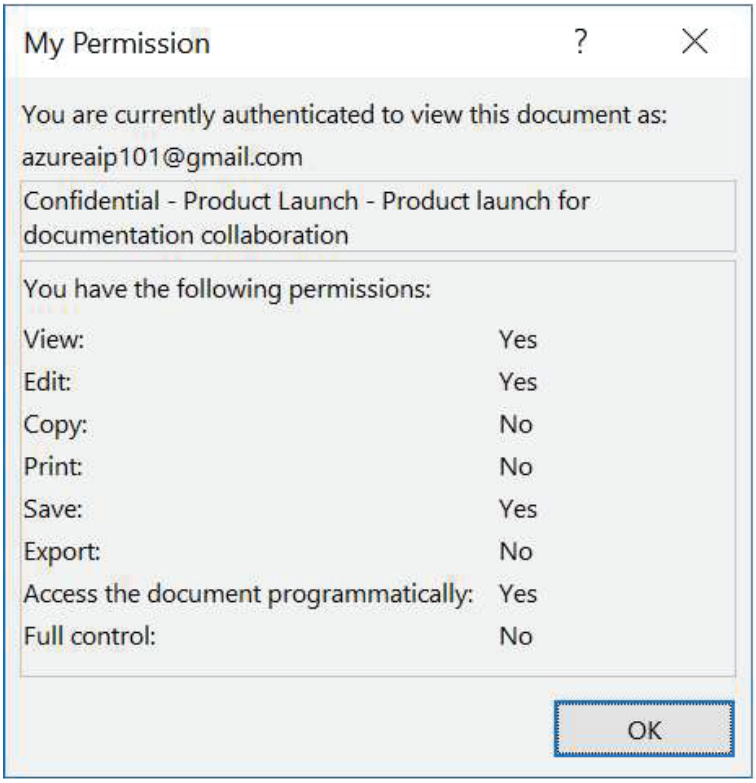
What's happening in step 1: The authenticated user sends the document policy and the user's certificates to the Azure Rights Management service. The service decrypts and evaluates the policy, and builds a list of rights (if any) the user has for the document. To identify the user, the Azure AD ProxyAddresses attribute is used for the user's account and groups to which the user is a member. For performance reasons, group membership is cached. If the user account has no values for the Azure AD ProxyAddresses attribute, the value in the Azure AD UserPrincipalName is used instead.

How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

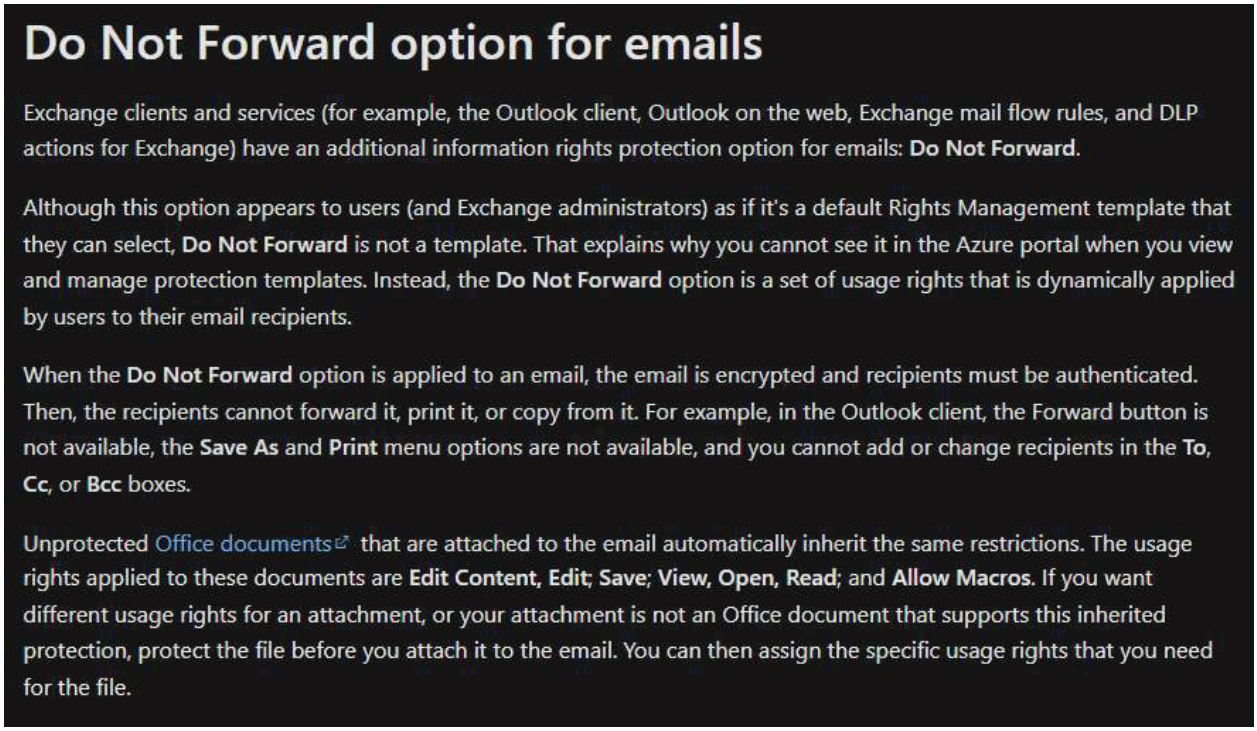
125. The authorized user comprises a user having a Content Consumer License (CCL) (e.g., use license / end user license) compatible with the PK to enable decryption of the encrypted content by the PK included within the PDP and use of decrypted content in accordance with advanced permissions (e.g. permissions to save, view, print, edit/modify, and/or forward) indicated via the CCL. *See* https://learn.microsoft.com/en-us/azure/information-protection/configure-usage-rights (last visited June 2023).



How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).



See https://learn.microsoft.com/en-us/previous-versions/azure/information-protection/secure-collaboration-documents#opening-and-editing-the-protected-document (last visited June 2023).



Do Not Forward option for emails

Exchange clients and services (for example, the Outlook client, Outlook on the web, Exchange mail flow rules, and DLP actions for Exchange) have an additional information rights protection option for emails: **Do Not Forward**.

Although this option appears to users (and Exchange administrators) as if it's a default Rights Management template that they can select, **Do Not Forward** is not a template. That explains why you cannot see it in the Azure portal when you view and manage protection templates. Instead, the **Do Not Forward** option is a set of usage rights that is dynamically applied by users to their email recipients.

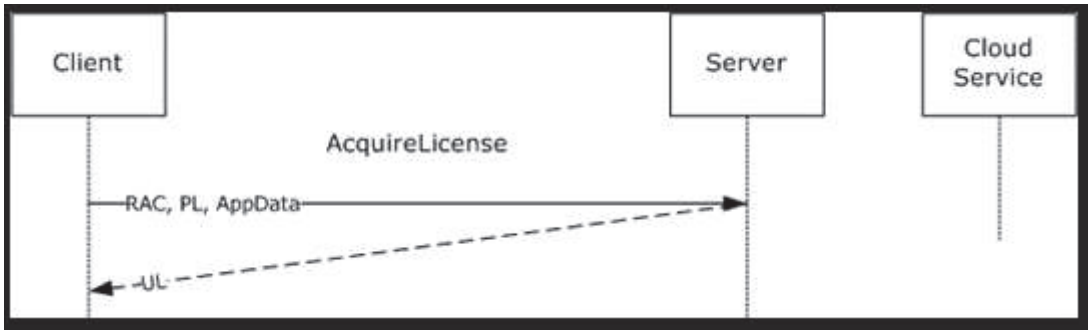
When the **Do Not Forward** option is applied to an email, the email is encrypted and recipients must be authenticated. Then, the recipients cannot forward it, print it, or copy from it. For example, in the Outlook client, the Forward button is not available, the **Save As** and **Print** menu options are not available, and you cannot add or change recipients in the **To**, **Cc**, or **Bcc** boxes.

Unprotected Office documents that are attached to the email automatically inherit the same restrictions. The usage rights applied to these documents are **Edit Content, Edit**; **Save**; **View, Open, Read**; and **Allow Macros**. If you want different usage rights for an attachment, or your attachment is not an Office document that supports this inherited protection, protect the file before you attach it to the email. You can then assign the specific usage rights that you need for the file.

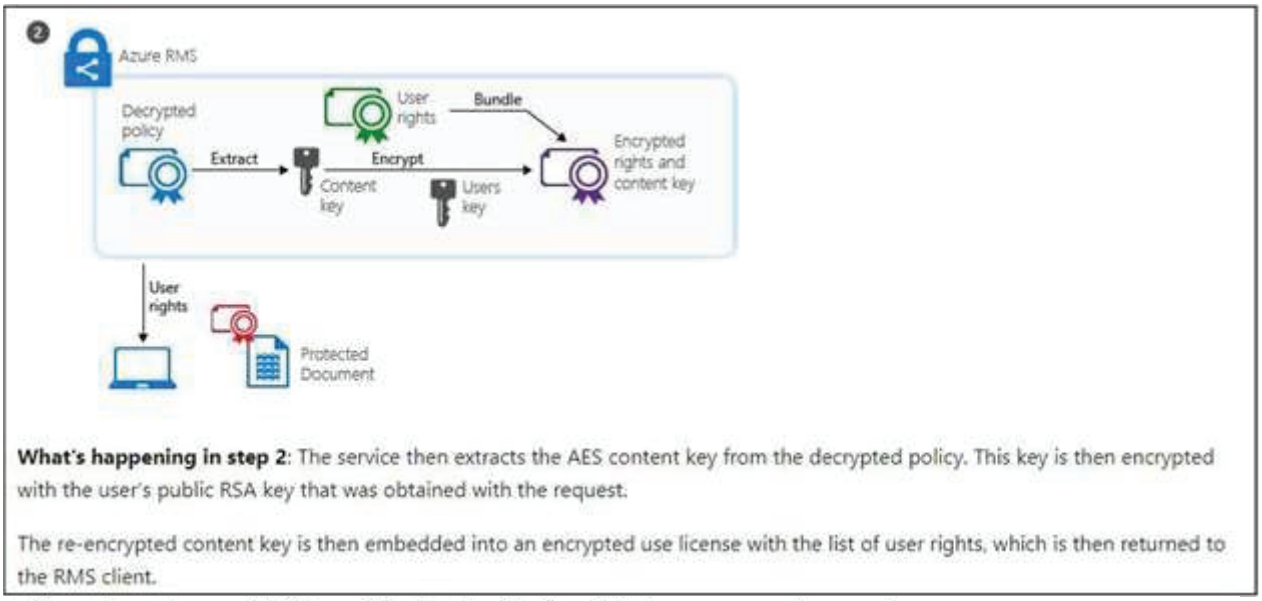
See https://learn.microsoft.com/en-us/azure/information-protection/configure-usage-rights (last visited June 2023).

126. The Microsoft Azure RMS Platforms propagate, via the network, the PDP toward at least one user.

127. In response to receiving from a proposed authorized user a CCLR identifying said PK, the Microsoft Azure RMS Platforms propagate a CCL compatible with the PK toward the proposed authorized user.



See https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-rmpr/2402901e-ee24-40fc-a480-5d007dbfdf57 (last visited June 2023).



How does Azure RMS work? Under the hood, MICROSOFT AZURE INFORMATION PROTECTION DOCUMENTATION, available at: https://docs.microsoft.com/en-us/azure/information-protection/how-does-it-work#walkthrough-of-how-azure-rms-works-first-use-content-protection-content-consumption (last visited April 2020).

128. On information and belief, one or more Microsoft subsidiaries and/or affiliates use the Microsoft Azure RMS Platforms in regular business operations.

129. On information and belief, the Microsoft Azure RMS Platforms are available to businesses and individuals throughout the United States.

130. On information and belief, the Microsoft Azure RMS Platforms are

provided to businesses and individuals located in the Western District of Texas.

131. On information and belief, Microsoft, without authorization or license, has been and continues to directly infringe (literally and/or under the doctrine of equivalents) at least claim 1 of the '848 patent by making, using, selling, offering for sale, and/or importing products, systems, offerings, and/or services for securely generating, distributing, and/or consuming content including, but not limited to, the Microsoft Azure RMS Platforms.

132. For example, in the context of protected documents on the Microsoft Azure RMS Platforms, specific email addresses or domains can be added to a rights policy template. Those email addresses are external to the organization of the content owner or sender (e.g., outside the content owner's/sender's domain) and have not been federated with the domain of the content owner/sender prior to sending the protected document. Thus, infringement occurs at least by Microsoft implementing the feature shown in the red box below.

- Any email address or domain. Use this option to specify all users in another organization who uses Azure AD, by entering any domain name from that organization. You can also use this option for social providers, by entering their domain name such as **gmail.com**, **hotmail.com**, or **outlook.com**.

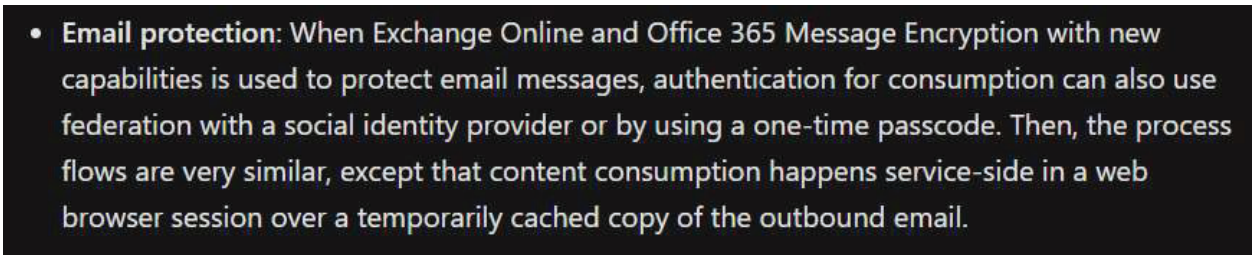
See https://learn.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels?view=o365-worldwide#requirements-and-limitations-for-add-any-authenticated-users (last visited June 2023).

133. As another example, in the context of protected emails (including email attachments) on the Microsoft Azure RMS Platforms, specific email addresses or domains—which are external to the organization of the content owner or sender (e.g.,

outside the content owner's/sender's domain) and have not been federated with the domain of the content owner/sender—can be added to a rights policy template. Thus, infringement occurs at least by: (1) sending a protected email between a Microsoft email application (web, mobile, or desktop) and (a) a Microsoft email web application (e.g., Outlook web application (OWA)) or (b) a non-Microsoft application (e.g. Gmail, Yahoo! MacOS mail, and other web and/or desktop mail applications); or (2) sending a protected email between a Microsoft email application (web, mobile, or desktop) and a non-Microsoft mobile application (e.g. Gmail, iOS mail).

Situation	Legacy OME	IRM in AD RMS	Microsoft Purview Message Encryption
Sending an encrypted mail	Through Exchange mail flow rules	End-user initiated from Outlook desktop or Outlook on the Web; or through Exchange mail flow rules	End-user initiated from Outlook desktop, Outlook for Mac, or Outlook on the Web; through Exchange mail flow rules (also known as transport rules) and data loss prevention (DLP)
Rights management template	N/A	Do Not Forward option and custom templates	Do Not Forward option, encrypt-only option, and custom templates
Recipient type	Internal and external recipients	Internal recipients only	Internal and external recipients
Experience for internal recipient	Recipients receive an HTML message, which they download and open in a web browser or mobile app	Native inline experience in Outlook clients	Native inline experience for recipients in the same organization using Outlook clients. Recipients can read message from encrypted message portal using clients other than Outlook (no download or app required).
Experience for external recipient	Recipients receive an HTML message, which they download and open in a web browser or mobile app	N/A	Native inline experience for Microsoft 365 recipients. All other recipients can read message from OME portal (no download or app required).
Attachment permissions	No restrictions on attachments	Attachments are protected	Attachments are protected for the Do Not Forward option and custom templates. Admins can choose whether attachments for the encrypt-only option are protected or not.
Bring your own key (BYOK) support	None	None	BYOK supported

See https://learn.microsoft.com/en-us/microsoft-365/compliance/ome-version-comparison?view=o365-worldwide (last visited June 2023).



See https://learn.microsoft.com/en-us/azure/information-protection/how-does-it-work (last visited June 2023).

See https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/secure-email-recommended-policies?view=o365-worldwide (last visited June 2023).

134. By making, using, offering for sale, selling, and/or importing products, systems, offerings, and/or services for securely generating, distributing, and/or consuming protected content (including, but not limited to, the Microsoft Azure RMS Platforms), Microsoft has injured paSafeShare and is liable to the Plaintiff for directly infringing one or more claims of the '848 patent, including at least claim 1 pursuant to 35 U.S.C. § 271(a)

135. On information and belief, Microsoft also indirectly infringes the '848

patent by actively inducing infringement under 35 USC § 271(b).

136. Microsoft has been on notice of the '848 patent at least since November 9, 2019.

137. On information and belief, Microsoft intends/intended to induce patent infringement by third-party customers and users of the Microsoft Azure RMS Platforms and has/had knowledge that its inducing acts cause/would cause infringement or is/was willfully blind to the possibility that its inducing acts cause/would cause infringement.

138. On information and belief, Microsoft specifically intends and is aware that the normal and customary use of the accused products infringe the '848 patent. Microsoft performs the acts that constitute induced infringement, and induces actual infringement, with knowledge of the '848 patent and with the knowledge that the induced acts constitute infringement. For example, Microsoft provides the infringing Microsoft Azure RMS Platforms, and further provides documentation and training materials that cause customers and end users of the Microsoft Azure RMS Platforms to use the products in a manner that directly infringe one or more claims of the '848 patent. By providing instruction and training to customers and end users on how to use the Microsoft Azure RMS Platforms in a manner that directly infringes one or more claims of the '848 patent, including at least claim 1, Microsoft specifically intends to induce infringement of the '848 patent. On information and belief, Microsoft engages in such inducement (e.g., through Microsoft user manuals, product support, marketing materials, and training materials to actively induce the users of the Microsoft Azure

RMS Platforms to infringe the '848 patent) to promote the sales of the Microsoft Azure RMS Platforms. Accordingly, Microsoft has induced and continues to induce users of the Microsoft Azure RMS Platforms to use the Microsoft Azure RMS Platforms in their ordinary and customary way to infringe the '848 patent, knowing that such use constitutes infringement of the '848 patent.

139. Microsoft's infringement of the '848 patent was and continues to be willful.

140. Microsoft's direct and/or indirect infringement has damaged paSafeShare and paSafeShare is suffering and will continue to suffer irreparable harm and damages as a result of this infringement.

JURY DEMANDED

141. Pursuant to Federal Rule of Civil Procedure 38(b), paSafeShare requests a trial by jury on all issues so triable.

PRAYER FOR RELIEF

paSafeShare respectfully requests this Court to enter judgment in paSafeShare's favor and against Microsoft as follows:

a. finding that Microsoft has infringed one or more claims of the '961 patent;

b. finding that Microsoft has infringed one or more claims of the '116 patent;

c. finding that Microsoft has infringed one or more claims of the '848 patent;

d. finding that Microsoft's infringement was willful;

e. awarding paSafeShare damages under 35 U.S.C. § 284, or otherwise permitted by law, including supplemental damages for any continued

post-verdict infringement and enhanced damages in view of Microsoft's willful infringement;

f. awarding paSafeShare pre-judgment and post-judgment interest on the damages award and costs;

g. awarding cost of this action (including all disbursements) and attorney fees pursuant to 35 U.S.C. § 285, or as otherwise permitted by the law; and

h. awarding such other costs and further relief that the Court determines to be just and equitable.

Dated: June 20, 2023

/s/ Raymond W. Mort, III
Raymond W. Mort, III
Texas State Bar No. 00791308
raymort@austinlaw.com
THE MORT LAW FIRM, PLLC
501 Congress Avenue, Suite 150
Austin, Texas 78701
Tel/Fax: 512-865-7950

Of Counsel:
Ronald M. Daignault (*pro hac vice*)*
Chandran B. Iyer (*pro hac vice*)
Jason S. Charkow (*pro hac vice)**
Scott R. Samay (*pro hac vice*)*
Shailendra Maheshwari (*pro hac vice)**
Stephanie R. Mandir (*pro hac vice)*
Zachary H. Ellis
(Texas State Bar No. 24122606)*
Kevin H. Sprenger (*pro hac vice)*
rdaignault@daignaultiyer.com
cbiyer@daignaultiyer.com
jcharkow@daignaultiyer.com
ssamay@daignaultiyer.com
smaheshwari@daignaultiyer.com
smandir@daignaultiyer.com
zellis@daignaultiyer.com
ksprenger@daignaultiyer.com
DAIGNAULT IYER LLP
8618 Westwood Center Drive, Suite 150
Vienna, Virginia 22182
**Not admitted in Virginia*

Attorneys for Plaintiff paSafeShare LLC